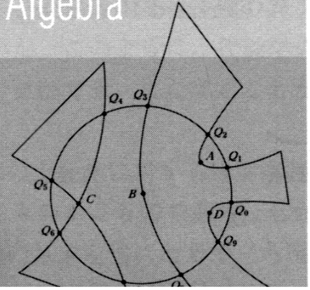
代数学の基本定理

The Fundamental Theorem of Algebra



Benjamin Fine
Gerhard Rosenberger 著
新妻　弘
木村哲三　訳

共立出版

The Fundamental Theorem of Algebra

Benjamin Fine Gerhard Rosenberger

序　文

この本は，アメリカ合衆国とドイツにおいて行った代数学の基本定理についての 2 つの講義から生まれた．これらの講義の目的は，初等数学とはいえないいくつかの分野を一つの話題を中心として呈示することにあった．代数学の基本定理はこの目的に対して理想的なものであった．解析学，代数学，そして位相数学の各分野は，それぞれこの基本定理を巡ってさまざまな技法を発展させてきた．それらの技法はこの重要な基本定理の異なった種々の証明方法と種々の視野へと我々を導いた．このように，代数学の基本定理によって多くの数学の分野を紹介することができ，また学ぶことができるということは驚くべきことである．

アメリカ合衆国においては学部の上級生に対する特別講義として行われた．話題の多くは学生達にとってなじみのあるものであり，しかしまたその多くは新しいものでもあった．代数学の基本定理にたえず立ち戻るという目標は，一見したところ関連のない題材に 1 つの焦点を与えた．さらに，5 次方程式の代数的不可解性や自然対数の底 e と 円周率 π が超越的であるというような，たくさんの良い応用例を紹介することができた．このような特別講義における学部の学生達は，この本の理想的な読者であると感じられる．アメリカ合衆国の多くの学部は，概説講義の考えを採用している．それで，この本は大学院初級の学生に対しては基本的文献として役に立つだろう．また，代数の章，第 2, 3, 6, 7 章は他からの必要な部分を付け加えれば，学部の代数系の代替え的なコースとして，または代数系の補助コースとして使うことができると思われる．この講義の合衆国版では 1 つのセメスターで，いくつかを省略して第 1 章から 第 7 章における題材のほとんどを講義することができ

た．この本全体は 2 セメスターで比較的ゆっくりとしたペースで講義することができるだろう．

ドイツにおいては，この題材は教員志望のクラスに対して講義された．高校（すなわち，ドイツにおいてはギムナジウム）の先生は幅の広い数学的話題に触れておいたほうがよいと思われる．我々の題材はこれらの受講者に対するこの目的を満足していた．合衆国における同様な教員養成コースにおいても，この本が採用されることを私達は願うものである．ドイツにおける講義では，この本全体が 2 セメスターで講義された．

この本の原稿を非常に注意深く校正してくれた Nicole Isermann に感謝する．またこの本の予備的な版を読み，数多くの提案をしてくれた Kati Bencsath と Bruce Chandler にも感謝し，そして最後に，有益な助言をしてくれた Paul Halmos に感謝する．

Benjamin Fine,
Fairfield University, United States
Gerhard Rosenberger,
Universitäte Dortmund, Germany

訳者まえがき

序文において著者達が述べているように，代数学の基本定理がさまざまな切り口によってさまざまに証明されることを見ておくことは，幅の広い数学的話題に触れるという意味でも，あるいは数学の基本に触れるという意味でも，数学教師志望の学生達にとって望ましいことである．この思いは訳者二人が長年抱いていた思いと共通のものがあった．というのは，我々が学んだ東京理科大学は，東京物理学校と呼ばれていた時代から数多くの数学教師を世に送り出していることで有名であり，我々もそこで数学教師になるための教育を受けていた．さらに，訳者の一人は母校にとどまり，今でも数学教師志望の学生達の教育にあたっているからである．このことが本書翻訳の動機である．しかしながら，ピタゴラスの定理に数多くの証明があることが，数学好きの人々に喜ばれているように，本書の内容もまた数学好きの人々に喜ばれるのではないかと我々は感じている．

翻訳に際しては，原本に忠実にすることを心がけたが，重複していると思われる部分あるいはわかりにくいと思われる部分に必要最小限の修正をさせていただいた．また，原本にない注を必要最小限付け加え，さらに日本語で入手可能な参考文献を補った．

本書の翻訳の原稿を注意深く読み，数多くの有益な提案をしてくれた東京理科大学の松本年男先生に感謝する．また，出版に際しお世話になった共立出版(株)の只野真奈美氏に感謝する．

2002 年 1 月

訳者

目　次

第 1 章　序文と歴史的覚え書き **1**

第 2 章　複素数 **6**

2.1　体と実数体 6
2.2　複素数体 12
2.3　複素数の幾何学的表示 15
2.4　極形式とオイラーの等式 16
2.5　ベキと根に対するド・モアブルの定理 20

第 3 章　多項式と複素多項式 **25**

3.1　体上の多項式環 25
3.2　整除と多項式の一意分解性 28
3.3　多項式の根と因数分解 33
3.4　実多項式と複素多項式 34
3.5　代数学の基本定理——証明 1 37
3.6　代数学の基本定理の結果 39

第 4 章　複素解析学と解析関数 **43**

4.1　複素関数と解析性 43
4.2　コーシー・リーマンの微分方程式 49
4.3　等角写像と解析性 55

第 5 章　複素積分とコーシーの定理 62
5.1　線積分とグリーンの定理 62
5.2　複素積分とコーシーの定理 72
5.3　コーシーの積分公式とコーシーの評価式 77
5.4　リウヴィルの定理と代数学の基本定理——証明 2 82
5.5　いくつかの付加的な結果 84
5.6　複素解析学についての結論 85

第 6 章　体と拡大体 88
6.1　代数拡大 88
6.2　体への根の添加 96
6.3　最小分解体 100
6.4　置換と対称式 102
6.5　代数学の基本定理——証明 3 108
6.6　応用——自然対数の底 e と 円周率 π の超越性 110
6.7　対称式の基本定理 116

第 7 章　ガロア理論 122
7.1　ガロア理論展望 122
7.2　有限群からの準備 124
7.3　ガロア拡大 131
7.4　自己同型写像とガロア群 135
7.5　ガロア理論の基本定理 140
7.6　代数学の基本定理——証明 4 145
7.7　ガロア理論のいくつかの応用 146
7.8　$\mathbb{R}$ の代数拡大と結論 153

第 8 章　位相と位相空間 158
8.1　回転数と代数学の基本定理——証明 5 158
8.2　位相数学——その展望 161
8.3　連続性と距離空間 163
8.4　位相空間と同相写像 170
8.5　位相空間 172

第 9 章 代数的位相幾何学と最後の証明 **179**
9.1 代数的位相幾何学 179
9.2 群論——アーベル群 181
9.3 ホモトピーと基本群 187
9.4 ホモロジー理論と三角形分割 196
9.5 ホモロジーの計算 204
9.6 球のホモロジーとブラウアー次数 207
9.7 代数学の基本定理——証明 6 209
9.8 結論 212

付録 A ガウスのオリジナルの証明 **215**

付録 B コーシーの積分定理再訪 **220**

付録 C 代数学の基本定理のさらに 3 つの複素解析的証明 **229**

付録 D 代数学の基本定理のさらに 2 つの位相的証明 **234**

参考文献および引用文献 **238**

索 引 **241**

第1章

序文と歴史的覚え書き

代数学の基本定理とは，任意の複素係数の多項式は複素数の根をもつ，という定理である．この基本的な結果の最初の証明はガウスにより与えられているが，代数学の基本定理は数論と方程式論の交差するところに位置しており，数学の他の多くの分野にも現れる．この本の目的は，3 つの分野（代数，関数論，位相）から代数学の基本定理の証明を考察することである．各分野での最初の証明はかなり直接的であり，また初等的な数学と考えられる事柄にのみ依存している．しかしながら，これらの最初の証明は，基本定理がそれから直接的な結果として得られるような，より一般的理論へとおのずから成長することになる．そして，これらの一般的な理論はそれぞれの分野において代数学の基本定理の第 2 の証明を構成する．

複素多項式とは $a_0, a_1, \cdots, a_n$ を複素数，n を自然数とするとき，

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

という式で表される複素関数のことである．この多項式の**根** あるいは**ゼロ**とは，$P(z_0) = 0$ を満たす複素数 z_0 のことである．

基本定理にさまざまな証明が現れるのは複素多項式のさまざまな異なった特性に基づいている．第一に，複素多項式は複素関数である．すなわち，複素数 $\mathbb{C}$ から $\mathbb{C}$ への関数である．実多項式と同様に，複素多項式はいたるところで微分可能であることから，複素解析の言葉で**整関数**と呼ばれる関数の中の一部分である．この視点においては，代数学の基本定理は**リウヴィルの定**

理と呼ばれる一般的な定理から直接的に得られる．リウヴィルの定理によれば，複素平面上で有界な整関数は定数である．第 2 章と第 3 章では，複素数と複素多項式についての基本的な結果を紹介する．そして，これらを用いて上級の微積分学のみを利用している代数学の基本定理の証明を呈示する．この証明はリウヴィルの定理を暗示している．第 4 章と第 5 章では，リウヴィルの定理を導き出すために必要な複素関数論からの結果 —— 特に，複素関数の微分，解析関数，複素積分とコーシーの定理 —— を呈示する．これを用いて，代数学の基本定理の第 2 の証明を与える．

別の見方をすると，複素多項式は代数的な対象である．この視点においては，代数学の基本定理は次のように言い換えることが出来る．「複素数体は代数的に閉じている」．第 6 章では，代数拡大に関する結果を呈示し，奇数次の実数係数多項式は実数の根をもつということと，与えられた体 F 上の既約多項式 $f(x)$ に対して，$f(x)$ がその中で根をもつような F の拡大体 F^* が構成される，という事実にのみ基づく代数学の基本定理の証明を呈示する．この証明は次の一般化を暗示している．K を奇数次の多項式が根をもつような体とし，$i=\sqrt{-1}$ とすれば，$K(i)$ は代数的閉体である．この一般化の証明は必然的に**ガロア理論**を伴う．第 7 章では，この証明を理解するために必要とされる群論とガロア理論の基本的な結果を示す．

最後に，複素多項式は位相写像である．無限遠点を複素平面に添加すれば球面，すなわち**リーマン球面** S^2 を得る．任意の複素多項式 $P(z)$ に対して $P(\infty)=\infty$ であるから，$P(z)$ は連続写像 $P: S^2 \longrightarrow S^2$ と考えることができる．このような位相写像は**回転数**と呼ばれる数，S^2 上の曲線 C の像が S^2 へ写像されるとき，どれだけ回転するかということを示す数をもつ．関数 $f(z)=z^n$ は複素数 z を原点のまわりに回転させる．第 8 章では，はじめに関数 $f(z)=z^n$ の回転する性質を用いて代数学の基本定理を証明する．そして，このことは関数 $S^2 \longrightarrow S^2$ の回転数へ一般化され，これより再び代数学の基本定理が証明される．この最後の一般化を扱うために，点集合位相数学と代数的位相幾何学の両方におけるいくつかの基本的な考え方と技術を紹介しなければならない．これは，第 8 章と第 9 章で説明する．この最後の証明は最も発展した数学を必要としているので，セルフ・コンテインドであるとは言えない．

ここに我々が示した証明には，さまざまなバリエーションがある．一連の

付録において 6 つの追加的証明を与える．それらはこの本の本文で与えられたものと幾分異なっている．付録 A ではガウスの原第一証明の現代版を与える．付録 C では複素解析学から生じた 3 つの追加的証明を呈示する．これらは第 5 章で与えられたものよりもさらに精密なコーシーの定理の分析を必要とする．この分析は付録 B で与えられる．最後に付録 D で 2 つの追加的な位相的に動機づけられた証明を与える．これらの証明は回転数の概念に基づいているが，第 8 章，第 9 章で与えられたものとは異なっている．

読者は少なくともグリーンの定理までの高等微積分学を学習していることを仮定する．また，いくつかの抽象代数学，特に群，環，体の定義を勉強し，また線形代数学，特に一般的な体上のベクトル空間の抽象的な定義を学習していることを仮定する．以上の仮定のもとに，この本をできるだけ自習可能な本となるように努力した．しかしながら，我々の目的は代数学の基本定理の証明の理解に到達することにある．したがって，そのことに沿って直接的に得ることのできる結果のみを証明し，より難しい結果（ガロア理論の基本定理のような）を引用文献に委ねた．ここで，術語についての注意を 1 つ述べる．標準的な使い方において,「方程式は根をもつ」といい,「関数と多項式はゼロをもつ」という．しかしながら，歴史的には根という言葉は非常にしばしば代数学の基本定理と結びついて用いられてきた．それゆえ，この本を通して根という術語を使い，多項式 $P(z)$ の零点と多項式の方程式 $P(z)=0$ の根とを区別しない．

次数 n の多項式によるすべての方程式はちょうど n 個の根をもつ，という形によって最初に代数学の基本定理に言及したのはニュルンベルクの ロスであった．しかしながら，その予想は一般的には 1629 年にその結果を述べたジローに帰されている．そして，それは 1637 年に実根と虚根をも区別していたデカルトによって明瞭に述べられた．最初の代数学の基本定理の証明は 1746 年に，ダランベールによって公表された．けれども，ダランベールの証明には飛躍があった．そして，最初に完全な形で認められた証明はガウスによって 1797 年に，彼の学位論文の中で与えられた．この論文は 1799 年に出版された．興味深いことに現代の数学者達がガウスのオリジナルの証明を調べるとダランベールの証明の中におけるものと同じぐらいの欠陥があるということである．しかしながら， ガウスはそのような欠陥のない証明を他に 3 つ発表している．彼は 1816 年に第 2，第 3 の証明を発表したが，後に最初のもの

とは本質的に異なる解釈である最後の証明を 1849 年に提出した．

この本の主要部分ではガウスのオリジナルな証明には触れていない．この証明の概略は次のとおりである．任意の $z \in \mathbb{C}$ に対して $P(z)$ は複素数であり，$z = x + iy$ $(x, y \in \mathbb{R})$ であるから，$P(z) = u(x,y) + iv(x,y)$ が成り立つ．このとき，方程式 $u(x,y) = 0$ と $v(x,y) = 0$ は平面 $\mathbb{R}^2$ における曲線を表す．複素多項式 $P(z)$ に対して，上記の関数 $u(x,y), v(x,y)$ を注意深く調べることによって，ガウスは曲線 $u(x,y) = 0, v(x,y) = 0$ は共通解 (x_0, y_0) をもたなければならないことを示した．複素数 $z_0 = x_0 + iy_0$ はそのとき，$P(z)$ の根である．付録 A において，ガウスのオリジナルな証明の 1 つの解釈を呈示する．

代数学の基本定理は実際，方程式論の発展全体の中の 1 部分である．2 次方程式が解けることと 2 次方程式の本質的な根の公式は約 3600 年前バビロニア人たちによって知られていた．虚数の発見によって，2 次方程式の根の公式は，次数 2 の任意の $\mathbb{C}$ 上の多項式は $\mathbb{C}$ に根をもつ，ということを主張していることになる．16 世紀にイタリアの数学者タルターリャ は 3 次方程式を解くためにベキ根による同様の公式を発見した．現在ではこの **3 次方程式の根の公式**は，誤ってカルダノを記念し，**カルダノの公式**として知られている．カルダノはそれを 1545 年に公表した．この公式の初期の特別な形はフェッロによって発見された．カルダノの弟子フェラーリはこの公式を 4 次の多項式をベキ根によって解く公式へ拡張した．これら一連の公式によって，4 次またはそれ以下の複素多項式は複素数の根を必ずもつ，ということがわかった．17 世紀において，連続関数の初等的な性質によって，すべての奇数次の実多項式は実根をもたねばならない，ということが明らかになった．これらすべての結果は，1608 年にロスによって言及され，1629 年にジローによって予想された代数学の基本定理の正しさに真実味を与えていた．

カルダノの仕事より 19 世紀の初頭まで，5 次多項式に対する同様な公式を見い出そうとする試みがなされた．1805 年に ルフィニは，5 次の多項式による方程式は一般にベキ根によって解くことは出来ない，ということを証明した．それゆえ，次数 5 に対する類似の公式は存在しない[1]．アーベル が 1825 年から 1826 年に，そしてガロアが 1831 年にルフィニの結果を拡張し，一般に次数 5 またはそれ以上の次数の方程式はベキ根によって解くことはできな

[1] いくつかの文献によればルフィニの証明は完全なものではなかった．

いことを証明した．この研究の中で，ガロアは体の拡大の理論を確立し，それと群論との関係を明らかにした．これは**ガロア理論**として知られるようになった（第 7 章で論じる）．代数学の基本定理のより詳しい歴史はレンメルトによる論文 [R] に見ることができる．

第2章 複素数

2.1 体と実数体

F が体であることの定義を思い起こそう．集合 F が体であるとは，$+$ によって表される加法 $a+b$ と $\cdot$ または単に並置して表される乗法 ab の 2 つの 2 項演算をもち，その上で次の 9 つの公理を満たす集合のことである．

(1) 加法は可換である：$a+b=b+a$ $(a,b\in F)$.

(2) 加法は結合的である：$a+(b+c)=(a+b)+c$ $(a,b,c\in F)$.

(3) 0 によって表される加法の単位元が存在する：$a+0=a$ $(a\in F)$.

(4) F の任意の元 a に対して，$-a$ で表される加法の逆元が存在する：$a+(-a)=0$.

(5) 乗法は結合的である：$a(bc)=(ab)c$ $(a,b,c\in F)$.

(6) 乗法は加法に対して分配的である：$a(b+c)=ab+ac$ $(a,b,c\in F)$.

(7) 乗法は可換である：$ab=ba$ $(a,b\in F)$.

(8) 1 $(1\neq 0)$ によって表される乗法の単位元が存在する：$a1=1a$ $(a\in F)$.

(9) F の任意の元 a に対して，a^{-1} で表される乗法の逆元が存在する：$aa^{-1}=1$.

1 つの演算 $+$ をもち，その上で公理 (1) から (4) までを満たしている集合は**アーベル群**または**可換群**と呼ばれる．公理 (1) から (6) は**環**を定義し，(1) から (8) は**単位元をもつ可換環**を定義する．したがって，一般的な現代代数

学においては，体とは単位元をもち，0 ではないすべての元は乗法の逆元をもつ可換環として定義される．

体は，その中ですべての算術的な演算：加法，減法（加法の逆元を加えること），乗法，そして除法（乗法の逆元をかけること）を実行することができる最も基本的な代数的構造をもつものと考えられる．

体の例としては**有理数**の全体 $\mathbb{Q}$，任意の**素数** $\boldsymbol{p}$ **を法とする剰余類**の全体（これは $\mathbb{Z}_p$ によって表される），**実数**のつくる体 $\mathbb{R}$ などがある．体のもう 1 つの例は後で見るように，代数拡大により得られるもので，次のようなものがある：

例 2.1.1 次のような集合を考える．

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\ ;\ a, b \in \mathbb{Q}\}.$$

$\mathbb{Q}(\sqrt{2})$ 上で加法と乗法を代数的操作によって定義する；すなわち，$x = a + b\sqrt{2}, y = c + d\sqrt{2}$ に対して，

$$\begin{aligned} x + y &= (a + c) + (b + d)\sqrt{2} \\ xy &= (ac + 2bd) + (bc + ad)\sqrt{2} \end{aligned}$$

とする．$\mathbb{Q}(\sqrt{2})$ が体であることを示すためには，性質 (1) から (9) を示さなければならない．これらの大部分を演習問題として残し，ここでは 0 でない元が乗法の逆元をもつことのみを証明しよう．

最初に，$\mathbb{Q}$ を $\{a + 0\sqrt{2}\ ;\ a \in \mathbb{Q}\}$ と同一視すれば，$\mathbb{Q}$ は $\mathbb{Q}(\sqrt{2})$ の部分集合と考えることができる．加法と乗法の定義より，$0 \in \mathbb{Q}$ と $1 \in \mathbb{Q}$ はそれぞれ，$\mathbb{Q}(\sqrt{2})$ における加法と乗法の単位元である．さて，$x = a + b\sqrt{2}, x \neq 0$ と仮定する．そのとき，a と b は 2 つとも 0 ではない．$\sqrt{2}$ は有理数ではないから $a^2 - 2b^2 \neq 0$ である．$\bar{x} = a - b\sqrt{2}$ とおく．簡単な計算によって，

$$x\bar{x} = a^2 - 2b^2.$$

そこで，

$$y = \frac{\bar{x}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2}$$

とおく．$a^2-2b^2\neq 0$ であるから，y の値は矛盾なく定義される．計算によって，$xy=1$ が成り立つことがわかるので，y は x の乗法逆元である．

この例は，d を完全平方でない有理数とするとき，$\mathbb{Q}(\sqrt{d})$ に対して一般化される．　□

F_1 が体 F の部分集合であり，F と同じ演算（加法と乗法），同じ単位元 (1 と 0) に関して体であるとき，F_1 は F の**部分体**といい，また F は F_1 の**拡大体**であるという．たとえば，$\mathbb{Q}$ は $\mathbb{Q}(\sqrt{2})$ の部分体であり，$\mathbb{R}$ の部分体でもある．

F_1 が体 F の空でない部分集合であれば，それは自動的に結合律，可換律，分配律を満たす．したがって，それが加法と乗法に関して閉じており，0 と 1 を含み，その中で任意の元に対する加法の逆元および 0 でない任意の元に対する乗法の逆元を含んでいれば部分体となる．このことを次のように要約することができる．部分体 F_1 は加法，乗法，減法そして，除法に関して閉じていなければならない．このとき，F_1 は自動的に 0 と 1 を含んでいる．

定理 2.1.1　$F_1\subset F$ が部分体であるための必要十分条件は $F_1\neq\emptyset$ であって，F_1 が加法，乗法，減法そして，除法に関して閉じていることである．

例 2.1.2　$\mathbb{Q}(\sqrt{2})$ は $\mathbb{R}$ の部分体であり，したがって体であることを示せ．

例 2.1.1 において，$\mathbb{Q}(\sqrt{2})$ は体であることを示した．ここでは，定理 2.1.1 を使って同じことを示そう．

さて，$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})$ であるから，$\mathbb{Q}(\sqrt{2})\neq\emptyset$ である．したがって，$\mathbb{Q}(\sqrt{2})$ が体であることを示すには，それが 4 つの算術的演算に関して閉じていることを示さなければならない．そこで，$x=a+b\sqrt{2}, y=c+d\sqrt{2}$ $(a,b,c,d\in\mathbb{Q})$ で $y\neq 0$ と仮定する．すると，

$$\begin{aligned}
x\pm y &= (a\pm c)+(b\pm d)\sqrt{2}\in\mathbb{Q}(\sqrt{2})\\
&\quad(\because\ a\pm c\in\mathbb{Q},\ b\pm d\in\mathbb{Q})\\
xy &= (ac+2bd)+(bc+ad)\sqrt{2}\in\mathbb{Q}(\sqrt{2})\\
&\quad(\because\ ac+2bd\in\mathbb{Q},\ bc+ad\in\mathbb{Q})\\
1/y &= \frac{c}{c^2-2d^2}-\frac{d\sqrt{2}}{c^2-2d^2}\in\mathbb{Q}(\sqrt{2})\\
&\quad\left(\because\ \frac{c}{c^2-2d^2}\in\mathbb{Q},\ \frac{d}{c^2-2d^2}\in\mathbb{Q}\right)
\end{aligned}$$

上式の後の 2 つの事実より，x/y は $\mathbb{Q}(\sqrt{2})$ に属していることがわかる．したがって，$\mathbb{Q}(\sqrt{2})$ は空集合ではなく，算術的演算に関して閉じているので，それは $\mathbb{R}$ の部分体である． □

V が体 F 上の**ベクトル空間**であるということの定義を思い起こそう．V が体 F 上のベクトル空間であるとは，V がアーベル群であり次の条件を満たす V の元 v と F の元 f とのスカラー乗法 $fv \in V$ をもつということである．

(1) $f \in F, v \in V$ ならば $fv \in V$.
(2) $f(u+v) = fu + fv \quad (f \in F,\ u, v \in V)$.
(3) $(f+g)v = fv + gv \quad (f, g \in F,\ v \in V)$.
(4) $(fg)v = f(gv) \quad (f, g \in F,\ v \in V)$.
(5) $1v = v \quad (v \in V)$.

F_1 が F の部分体であれば，F の元に F_1 の元をかけた積はまた F の元である．F は加法に関してアーベル群であるから，F は F_1 上のベクトル空間として見ることができる．以上のようにして，どんな拡大体もその任意の部分体上のベクトル空間である．F が F_1 の拡大体であるとき，F_1 上のベクトル空間としての F の次元は**拡大次数**と呼ばれる．

例 2.1.3

(1) $\mathbb{Q}$ 上 $\mathbb{Q}(\sqrt{2})$ の拡大次数は 2 である．なぜなら，$\{1, \sqrt{2}\}$ は基底であるから．
(2) $\mathbb{R}$ は $\mathbb{Q}$ 上 無限次元の拡大体である．なぜなら，$\mathbb{R}$ は $\mathbb{Q}$ 上 無限次元であるから． □

この例の (2) の事実は**超越数**の存在に基づいている．元 $r \in \mathbb{R}$ は，それが $\mathbb{Q}$ に係数をもつゼロでない多項式を満足しているとき，$\mathbb{Q}$ 上**代数的**であるという．すなわち，

$$0 \neq P(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_i \in \mathbb{Q}$$

なる多項式が存在して，$P(r) = 0$ が満たされるとき，r は $\mathbb{Q}$ 上代数的であるといわれる．任意の $q \in \mathbb{Q}$ は，$P(x) = x - q$ とおけば $P(q) = 0$ であるか

ら，$\mathbb{Q}$ 上代数的である．さらに，たくさんの無理数もまた代数的である．たとえば，$x^2-2=0$ は $\sqrt{2}$ を根としてもつ．よって，$\sqrt{2}$ は $\mathbb{Q}$ 上代数的である．元 $r \in \mathbb{R}$ は代数的でないとき，**超越的**であるという．

一般に，ある特別な元が超越的であることを証明するのは非常に難しい．しかし，数えられないほどたくさんの超越数が存在する（演習問題参照）．特別な例は古くからなじみのある自然対数の底 e と円周率 π である．第6章でそれらの超越性の証明を与える．

e は超越的であるから，任意の自然数 n に対してベクトルの集合 $\{1, e, e^2, \cdots, e^n\}$ は $\mathbb{Q}$ 上1次独立である．なぜならば，もしそうでないとすると e が満たす多項式が存在することになるからである．したがって，$\mathbb{R}$ に $\mathbb{Q}$ 上1次独立なベクトルが無限にたくさんあることになる．これは，$\mathbb{R}$ が $\mathbb{Q}$ 上有限次の拡大次数のとき不可能である．

後でこれらのアイデアに立ち戻ることにして，今は代数学の基本定理にとって本質的なある特別な性質を満たしている実数体 $\mathbb{R}$ を綿密に調べてみなければならない．

まず最初に $\mathbb{R}$ は**順序体**である．この言葉は次のことを意味している．正の実数全体の集合 $\mathbb{R}^+$ は，加法と乗法によって閉じており，$\mathbb{R}$ は**三分法**の規則を満たしている．すなわち，$r \in \mathbb{R}$ とすれば $r \in \mathbb{R}^+$ であるか，$r=0$ であるか，または $-r \in \mathbb{R}^+$ のいずれか1つだけが成り立つ．これによって，$x-y \in \mathbb{R}^+$ のとき $x>y$ とおけば，$\mathbb{R}$ 上に順序を定義することができる．

順序体であるということは，ゼロでない元の平方は正であることを要請する．すなわち，$r \in \mathbb{R}^+$ であれば $r^2 \in \mathbb{R}^+$ であり，$-r \in \mathbb{R}^+$ であれば $r^2=(-r)^2 \in \mathbb{R}^+$ である．したがって，$\mathbb{R}$ の正の数のみが平方根をもつ．特に，$\sqrt{-1}$ は $\mathbb{R}$ の中に存在しない．

例 2.1.4　$\mathbb{Q}$ も $\mathbb{R}$ の他の任意の順序体と同様に順序体である．しかしながら，素数を法とする整数 $\mathbb{Z}_p$ はそうではない．加法と乗法に関して閉じていて，三分法の規則を満たしている正の元の集合を含めばその体は必然的に無限集合となる．したがって，順序体は無限集合でなければならない．しかるに，$\mathbb{Z}_p$ は有限集合であるから，順序体ではない．□

次に $\mathbb{R}$ は**アルキメデス的**である．$\mathbb{R}^+$ の任意の元 x, y に対して $nx>y$ を

満たす自然数 n が存在するとき，$\mathbb{R}$ はアルキメデス的であるという．$\mathbb{Q}$ もまたアルキメデス的である．

最後に $\mathbb{R}$ は**完備**である．すなわち，$\mathbb{R}$ は**制限完備性** (LUB: Least Upper Bound) と呼ばれる性質を満たす．

制限完備性

実数 $\mathbb{R}$ の部分集合 S が上に有界であれば，S は上限 s_0 をもつ．すなわち，すべての $s \in S$ に対して $s \leq s_0$ であり，すべての $s \in S$ に対して $s \leq s_1$ ならば，$s_0 \leq s_1$ を満たす．

この制限完備性は，実数に対する完備性の定義として採用されている以下の 2 つの性質のいずれとも同値である．

コーシー列の収束性

$\{x_n\}$ が $\mathbb{R}$ におけるコーシー列でならば，$\{x_n\}$ は収束する．$\{x_n\}$ が**コーシー列**であるとは，任意の正数 ϵ に対して，ある番号 N が存在して，すべての $m, n > N$ に対して，$|x_n - x_m| < \epsilon$ が成り立つことである．

区間縮小法の原理

$\{I_n\}$ が $I_{n+1} \subset I_n$ を満たす閉区間の列で，その区間の長さが 0 に収束するならば，すべての区間に共通なただ 1 つの点 x_0 が存在する．

$\mathbb{Q}$ は完備ではないことに注意しよう．集合 $S = \{q \in \mathbb{Q}\ ;\ q^2 < 2\}$ を考えてみる．そのとき，S は $\mathbb{Q}$ において 3 を上界としてもつ．しかし，S は $\mathbb{Q}$ に上限をもたない．もし，もったとすると，それは $\mathbb{R}$ における上限と一致しなければならず，この上限は無理数 $\sqrt{2}$ となるからである．

$\mathbb{R}$ の完備性によって，連続関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ に対する**中間値の定理**を証明することができる．

定理 2.1.2（中間値の定理）$f : [a, b] \longrightarrow \mathbb{R}$ を連続関数とする．$f(a) < k < f(b)$ であるか，または $f(a) > k > f(b)$ ならば，$f(c) = k$ を満たす $c \in (a, b)$ が存在する (連続関数はその任意の 2 つの値の間にある任意の値をとる)．

代数学の基本定理にとって重要なのは次の系である．

系 2.1.1　$f:[a,b]\longrightarrow\mathbb{R}$ を連続関数で $f(a)f(b)<0$ と仮定する．そのとき，$a<c<b$ なる $c\in\mathbb{R}$ が存在して $f(c)=0$ を満たす．

この系を示すためには，式 $f(a)f(b)<0$ が $f(a)$ と $f(b)$ は異なる符号をとることを意味していることに注意しよう．一般性を失うことなく，$f(a)<0, f(b)>0$ と仮定してよい．そのとき，0 は $f(a)$ と $f(b)$ の間にあり，中間値の定理を適用することができる．

これらの特別な性質は**同型**を除いて完全に $\mathbb{R}$ を決定する．

R と S を環として，関数 $f:R\longrightarrow S$ が次の性質を満たしているとき，関数 f を**準同型写像**という．

(1) $f(r_1+r_2)=f(r_1)+f(r_2)\quad(r_1,r_2\in R)$.
(2) $f(r_1r_2)=f(r_1)f(r_2)\quad(r_1,r_2\in R)$.

f が準同型写像でかつ全単射であるとき，**同型写像**であるといい，R と S は**同型**であるという．同型である環の代数的構造は本質的に同じである．

定理 2.1.3　F を完備なアルキメデス的順序体とすると，F は実数体 $\mathbb{R}$ に同型である．

2.2　複素数体

実数 $\mathbb{R}$ の中には $\sqrt{-1}$ は存在しない．今，形式的に　$\boldsymbol{i}=\sqrt{-1}$ と定義しよう．$\boldsymbol{i}=\sqrt{-1}$, すなわち，$\boldsymbol{i}$ は $\boldsymbol{i}^2=-1$ を満たす新しい元である．歴史的に $\boldsymbol{i}$ は**虚数単位**と呼ばれているが，次節で見るように，$\boldsymbol{i}$ は非常に実際的な幾何学的意味をもっている．

複素数は $z=x+\boldsymbol{i}y\ (x,y\in\mathbb{R})$ という形の表現である．$x=0, y\neq 0$ でならば，z は $z=\boldsymbol{i}y$ という形であり，このとき，z は（純）**虚数**と呼ばれている．**複素数**の集合を $\mathbb{C}$ によって表せば，$\mathbb{C}$ は次のように表される．

$$\mathbb{C}=\{x+\boldsymbol{i}y\ ;\ x,y\in\mathbb{R}\}.$$

実数 x を複素数 $x+0\boldsymbol{i}$ と同一視すれば，集合として $\mathbb{R}\subset\mathbb{C}$ である．

$\boldsymbol{i}^2 = -1$ という事実を用いて，$\mathbb{C}$ 上に算術演算を代数的な細工によって定義する．すなわち，$z = x + \boldsymbol{i}y$, $w = a + \boldsymbol{i}b$ として次のように決める．

(i) $z \pm w = (x \pm a) + \boldsymbol{i}(y \pm b)$.

(ii) $zw = (xa - yb) + \boldsymbol{i}(xb + ya)$.

$$(\because \quad \begin{aligned}(x + \boldsymbol{i}y)(a + \boldsymbol{i}b) &= xa + \boldsymbol{i}(ya) + \boldsymbol{i}(xb) + \boldsymbol{i}^2(yb) \\ &= (xa - yb) + \boldsymbol{i}(xb + ya)\,).\end{aligned}$$

例 2.2.1 $z = 3 + 4\boldsymbol{i}, w = 7 - 2\boldsymbol{i}$ とすれば，このとき：

(1) $z + w = 10 + 2\boldsymbol{i}$.

(2) $z - w = -4 + 6\boldsymbol{i}$.

(3) $zw = 29 + 22\boldsymbol{i}$. □

これらの定義のもとで，$\mathbb{C}$ が単位元をもつ可換環であり，$\mathbb{R}$ は $\mathbb{C}$ の部分環であることを確かめるのは容易である（演習問題参照）．ゼロは $0 \in \mathbb{R}$ であり，$0 + 0\boldsymbol{i}$ と同一視され，また乗法単位元は $1 \in \mathbb{R}$ であり，$1 + 0\boldsymbol{i}$ と同一視される．$\mathbb{C}$ が体であるためには，乗法の逆元をもたねばならない．乗法の逆元をどのように構成するか調べてみよう．

定義 2.2.1 $z \in \mathbb{C}$ を $z = x + \boldsymbol{i}y$ とするとき，z の**共役複素数** $\overline{z}$ とは $\overline{z} = x - \boldsymbol{i}y$ のことであり，また z の**絶対値** とは $|z| = \sqrt{x^2 + y^2}$ のことである．

例 2.2.2 $z = 3 + 4\boldsymbol{i}$ とすれば，$\overline{z} = 3 - 4\boldsymbol{i}$ であり，$|z| = \sqrt{9 + 16} = 5$.

次の補題は共役複素数と絶対値の性質を与えており，またこれより，逆元を構成することができる．

補題 2.2.1 $z, w \in \mathbb{C}$ とするとき，次が成り立つ．

(1) $|z| \geq 0$ である．$|z| = 0$ であるのは $z = 0$ であるときに限る．

(2) $|zw| = |z||w|$.

(3) $|z + w| \leq |z| + |w|$.

これらの証明は簡単な計算により確かめられるので読者の演習問題とする．これらの性質はまさに実数の絶対値の性質そのものであり，それゆえ $\mathbb{C}$ 上の解析学を可能にする．

補題 2.2.2　$z, w \in \mathbb{C}$ とするとき，次が成り立つ．

(1) $\overline{z+w} = \overline{z} + \overline{w}$.

(2) $\overline{zw} = (\overline{z})(\overline{w})$.

(3) $\overline{\overline{z}} = z$.

(4) $|\overline{z}| = |z|$.

(5) $\overline{z} = z$ が成り立つのは z が実数であるときに限る．

(1) から (4) までは単なる計算である．(5) について，$z = x + \boldsymbol{i}y$ とする．このとき，$\overline{z} = x - \boldsymbol{i}y$ であり，$z = \overline{z}$ であるための必要十分条件は $y = -y$. これが可能なのは $y = 0$ のときだけであり，$z = x + 0\boldsymbol{i}$ で z は実数である．

さて次の式を考えよう．

$$z\overline{z} = (x + \boldsymbol{i}y)(x - \boldsymbol{i}y) = x^2 - \boldsymbol{i}^2 y^2 = x^2 + y^2 = |z|^2.$$

それで，次の結果が成り立つ．

補題 2.2.3　$z \in \mathbb{C}$ とするとき，$z\overline{z} = |z|^2$ である．

この補題によって，$z \neq 0$ であれば

$$z\frac{\overline{z}}{|z|^2} = \frac{|z|^2}{|z|^2} = 1$$

であり，次のように定義することができる．

定義 2.2.2　0 でない任意の複素数 z に対して $\dfrac{1}{z} = \dfrac{\overline{z}}{|z|^2}$ と定義する．

例 2.2.3　$z = 3 + 4\boldsymbol{i}, w = 7 - 2\boldsymbol{i}$ とすれば，

(1) $\dfrac{1}{z} = \dfrac{3 - 4\boldsymbol{i}}{3^2 + 4^2} = \dfrac{3}{25} - \dfrac{4}{25}\boldsymbol{i}$.

(2) $\dfrac{z}{w} = z\dfrac{1}{w} = (3 + 4\boldsymbol{i})\dfrac{7 + 2\boldsymbol{i}}{53} = \dfrac{13}{53} + \dfrac{34}{53}\boldsymbol{i}$.

定義により複素数に対して除法が成り立つことになったので，$\mathbb{C}$ は体である．

定理 2.2.1　$\mathbb{C}$ は体であり，$\mathbb{R}$ は $\mathbb{C}$ の部分体である．$\mathbb{C}$ は $\mathbb{R}$ の拡大体として，拡大次数は 2 である．さらに，$\mathbb{C}$ は順序体ではない．

$\mathbb{C}$ を $\mathbb{R}$ 上のベクトル空間としてみたとき，$\{1, \boldsymbol{i}\}$ が 1 つの基底であることが容易にわかる．これより，$\mathbb{R}$ 上 $\mathbb{C}$ の拡大次数は 2 であることがわかる．$\mathbb{C}$ は次の理由によって，順序体であることはない．任意の順序体 F においては，$1^2 = 1$ であるから 1 は正の数である．しかしそのとき，三分法によって -1 は負の数でなければばらない．したがって，前の節で説明したように，-1 は平方根をもつことができない．

2.3 複素数の幾何学的表示

各複素数 $z = x + \boldsymbol{i}y$ を xy-平面 $\mathbb{R}^2$ における点 (x, y) と同一視することができる．また逆に，各点 $(x, y) \in \mathbb{R}^2$ を複素数 $z = x + \boldsymbol{i}y$ と同一視することができる．このようにして，$\mathbb{R}^2$ が複素数から構成されていると考えるとき，$\mathbb{R}^2$ は**複素平面**と呼ばれる．

別の見方をすると，複素数 $z = x + \boldsymbol{i}y$ はベクトル $\overrightarrow{v} = (x, y)$ と見ることもできる．すなわち，原点 $(0, 0)$ を始点とし (x, y) を終点とするベクトルである．この表現では，絶対値の記号 $|\ |$ は単なるベクトル (x, y) の大きさであり，これはちょうど点 (x, y) から原点までの距離である．共役複素数 $\overline{z} = x - \boldsymbol{i}y$ には点 $(x, -y)$ が対応し，この点は x 軸に関して (x, y) に対称な点である．

例 2.3.1 (図 2.1 参照) この幾何学的表示によって算術的操作を表現すること

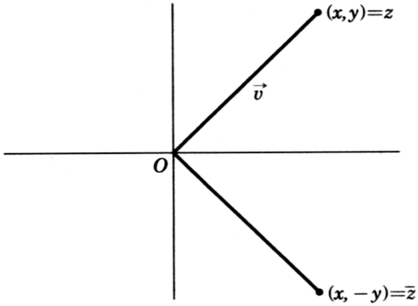


図 2.1 幾何学的表示

とができる．加法と減法は成分ごとになされるから，複素数の加法と減法は図 2.2 の中で描かれたベクトルの加法と減法に対応している．

例 2.3.2 複素数に実数をかけることは 2 次元ベクトルのスカラー乗法である．

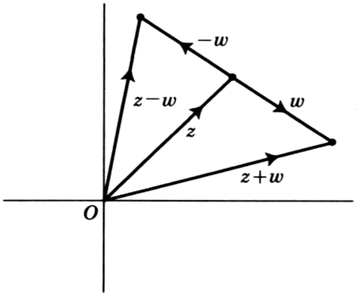


図 **2.2**　ベクトル演算

これは幾何学的には**拡大**することである．すなわち，$z \in \mathbb{C}, r \in R$ とすれば，

(1) $r \geq 0$ のとき，$rz = w$ とおけば w は大きさ $|r||z|$ をもち，z と同じ方向のベクトルである．

(2) $r < 0$ のとき，$rz = w$ とおけば w は大きさ $|r||z|$ をもち，z と反対方向のベクトルである．

$z = x + \boldsymbol{i}y$ ならば，$\boldsymbol{i}z = -y + \boldsymbol{i}x$ である．すなわち，$\boldsymbol{i}$ をかけるということは点 (x, y) を点 $(-y, x)$ に移すことである．内積をとると，$\langle (x, y), (-y, x) \rangle = -xy + xy = 0$ であるから，これらのベクトルは直交している．$1\boldsymbol{i} = \boldsymbol{i}$ であるから，虚数単位 $\boldsymbol{i}$ をかけることは時計と反対回りに 90 度回転させることに対応している．それゆえ，$\boldsymbol{i}$ はいかなる意味においても「非現実的」なものではなく，それは回転に対応している．

以上のことを総合して，複素数の積に対して，完全な幾何学的説明を与えることができる．$z, w \in \mathbb{C}$, $z = x + \boldsymbol{i}y$ として，$zw = (x + \boldsymbol{i}y)w = xw + \boldsymbol{i}yw$ を考察する．このとき，最初にベクトル w を x 倍拡大，次にベクトル w を y 倍拡大し，この 2 番目に拡大したベクトルを 90 度だけ左回りに回転する．最後に，それらのベクトルを加える（図 2.3 参照）．

2.4　極形式とオイラーの等式

$P \in \mathbb{R}^2$ の直交座標を (x, y) とすると，一方で P は**極座標** (r, θ) をもつ．ただし，r は原点 O から P への距離であり，θ はベクトル $\overrightarrow{OP}$ が正の x 軸となす角である (図 2.4 参照).

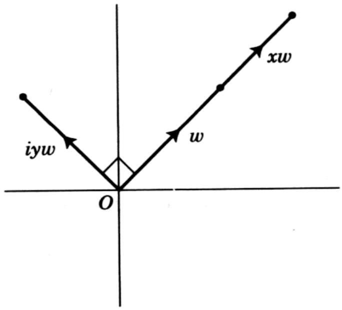


図 **2.3** 複素数の乗法

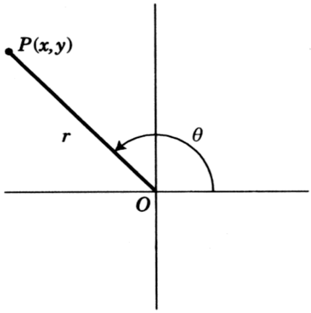


図 **2.4** 極形式

ここで，θ を領域 $[0, 2\pi)$ に制限すれば，$\mathbb{R}^2$ における各点はただ 1 つの極座標をもつ．点 P の直交座標 (x, y) は次の公式によってその極座標 (r, θ) と結びつけられる．

(i) $x = r\cos\theta.$

(ii) $y = r\sin\theta.$ (2.4.1)

(iii) $r = \sqrt{x^2 + y^2}.$

(iv) 適当な四分円の中で選ばれた $\theta = \arctan\dfrac{y}{x}.$

$z = x + \boldsymbol{i}y$ が極座標として (r, θ) をもつ点 (x, y) に対応しているとすれば，式 (2.4.1) から z は次のように表現することができる．

$$z = r(\cos\theta + \boldsymbol{i}\sin\theta). \tag{2.4.2}$$

これは z の**極形式**と呼ばれている．角度 θ を z の**偏角**といい，$\operatorname{Arg} z$ と表される．そして，この文脈のなかでは $|z|$ は z の**係数**と呼ばれる．

例 2.4.1 $z=1-\boldsymbol{i}$ とすると，$|z|=\sqrt{2}$ であり，$(1,-1)$ は第 4 象限にあるから $\mathrm{Arg}\, z=\arctan(-1)=\dfrac{7}{4}\pi$. したがって，$z=\sqrt{2}/\cos\dfrac{7}{4}\pi+\boldsymbol{i}\sin\dfrac{7}{4}\pi))$. と表される． □

極形式を表すための非常に良い，オイラーによる指数的表現方法がある．これを説明する前に，$\boldsymbol{i}$ のベキをもう少し調べてみなければならない．

さて，$\boldsymbol{i}^2=-1$ であるから，$\boldsymbol{i}^3=\boldsymbol{i}^2\boldsymbol{i}=-\boldsymbol{i}$. そして，$\boldsymbol{i}^4=\boldsymbol{i}^3\boldsymbol{i}=-\boldsymbol{i}^2=1$. したがって，$\boldsymbol{i}^5=\boldsymbol{i}$ となる．以上よりわかることは，$\boldsymbol{i}$ のベキは巡回的に $\{1,\ \boldsymbol{i},\ -1,-\boldsymbol{i}\}$ を繰り返す．$\boldsymbol{i}^m=\boldsymbol{i}^n$ であるための必要十分条件は $n\equiv m \pmod 4$ である．たとえば，$\boldsymbol{i}^{51}=\boldsymbol{i}^3=-\boldsymbol{i}$. さらに，$\boldsymbol{i}$ の任意のベキの乗法の逆元はまた $\boldsymbol{i}$ のベキであるから，これらのベキの全体は乗法に関して群をなす．

補題 2.4.1 $\boldsymbol{i}$ のベキの全体は乗法に関して位数 4 の群をなす．

この命題は実際に，次の節で論じようしている 1 の原始 n 乗根に関する命題の特別な場合である．

t を変数としたとき，関数 $e^t, \sin t, \cos t$ は次のようなベキ級数展開をもつ．

$$\begin{aligned}
&(1)\ e^t=1+t+\frac{t^2}{2!}+\cdots+\frac{t^n}{n!}+\cdots.\\
&(2)\ \sin t=t-\frac{t^3}{3!}+\frac{t^5}{5!}-\cdots+(-1)^n\frac{t^{2n+1}}{(2n+1)!}+\cdots.\\
&(3)\ \cos t=1-\frac{t^2}{2!}+\frac{t^4}{4!}-\cdots+(-1)^n\frac{t^{2n}}{(2n)!}+\cdots.
\end{aligned}\tag{2.4.3}$$

さて，θ を実数として，$t=\boldsymbol{i}\theta$ を考え，これを式 (2.4.3) に代入すると $e^{\boldsymbol{i}\theta}$ を得る (t は実数ではないが，形式的に計算する)．$\boldsymbol{i}$ のベキに関する規則によって，

$$e^{\boldsymbol{i}\theta}=1+(\boldsymbol{i}\theta)+\frac{(\boldsymbol{i}\theta)^2}{2!}+\cdots=1+\boldsymbol{i}\theta-\frac{\theta^2}{2!}-\boldsymbol{i}\frac{\theta^3}{3!}+\cdots.$$

実数と虚数の部分に分けると，

$$\begin{aligned}
e^{\boldsymbol{i}\theta}&=(1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}+\cdots)+\boldsymbol{i}(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}+\cdots)\\
&=\cos\theta+\boldsymbol{i}\sin\theta.
\end{aligned}$$

これは**オイラーの等式**として知られている．

オイラーの等式

$$e^{\boldsymbol{i}\theta} = \cos\theta + \boldsymbol{i}\sin\theta \ (\theta \in \mathbb{R}).$$

今，$r = |z|, \theta = \mathrm{Arg}\ z$ とすれば，次の式が成り立つ．

$$z = r(\cos\theta + \boldsymbol{i}\sin\theta) = re^{\boldsymbol{i}\theta}. \tag{2.4.4}$$

この最後の等式によって複素数の乗法は非常に簡素化される．というのは，$z = r_1 e^{\boldsymbol{i}\theta_1}$，$w = r_2 e^{\boldsymbol{i}\theta_2}$ とするとき，$zw = r_1 r_2 e^{\boldsymbol{i}(\theta_1+\theta_2)}$ となるからである．これを各成分に分解して考えれば，$|zw| = |z||w|$ と $\mathrm{Arg}\ (zw) = \mathrm{Arg}\ z +\ \mathrm{Arg}\ w$ を得る．

補題 2.4.2　$z, w \in \mathbb{C}$ とすると，$|zw| = |z||w|$　と　$\mathrm{Arg}\,(zw) = \mathrm{Arg}\,z + \mathrm{Arg}\,w$ が成り立つ．

$\mathrm{Arg}\ \boldsymbol{i} = \pi/2$ であることに注意すれば，乗法 $\boldsymbol{i}z$ は z を 90 度回転させることである．すなわち，$\mathrm{Arg}\,(\boldsymbol{i}z) = \pi/2 + \mathrm{Arg}\,z = \mathrm{Arg}\,\boldsymbol{i} + \mathrm{Arg}\,z$ であって，これは補題より直接得られる．

オイラーの等式によって，直接**オイラーの魔法の等式**と呼ばれているものを導きだすことができる．$\theta = \pi$ とおけば，

$$e^{\boldsymbol{i}\pi} = \cos\pi + \boldsymbol{i}\sin\pi = -1 + 0\boldsymbol{i} = -1.$$

簡潔に書けば $e^{\boldsymbol{i}\pi} + 1 = 0$ である．

オイラーの魔法の等式

$$e^{\boldsymbol{i}\pi} + 1 = 0.$$

この等式は数学における 5 つの最も重要な数 0, 1, e, $\boldsymbol{i}$, π が非常に簡潔な 1 つの等式の中で密接に結びつけられている，という理由でオイラーの「魔法」の等式と呼ばれてきた．これらの数がいかに多様な形で —— 0 は加法の単位元として，1 は乗法の単位元として，e は自然対数の底として，π は円の直径に対する円周の比として —— 出現したかということを考えれば，この結果は真に驚くべきことである．

2.5　ベキと根に対するド・モアブルの定理

$z = re^{i\theta} \in \mathbb{C}$ とすれば，$n \in \mathbb{N}$ に対して，$z^n = r^n e^{in\theta}$ が成り立つ．このとき，$|z^n| = |z|^n$, $\mathrm{Arg}\,(z^n) = n\ \mathrm{Arg}\ z$ が成り立つことに注意しよう．これは，**ベキに対するド・モアブルの定理**として知られている．

ベキに対するド・モアブルの定理

$z = re^{i\theta} \in \mathbb{C}$ とすれば，$n \in \mathbb{N}$ に対して，$z^n = r^n e^{in\theta}$ が成り立つ．特に，$|z^n| = |z|^n$, $\mathrm{Arg}\,(z^n) = n\ \mathrm{Arg}\ z$ となっている．

例 2.5.1　$z = 1 - i$ として，z^{10} を求めてみよう．

今，$|z| = \sqrt{2}$, $\mathrm{Arg}\ z = 7\pi/4$ であるから，$z = \sqrt{2}e^{i\frac{7}{4}\pi}$ である．したがって，$z^{10} = \sqrt{2}^{10} e^{i\frac{70}{4}\pi}$．ここで，$(\sqrt{2})^{10} = 32$ であり，一方 $70\pi/4 = 16\pi + 3\pi/2 \equiv 3\pi/2$ (角として) である．以上より，

$$z^{10} = 32e^{i\frac{3}{2}\pi} = 32(\cos\frac{3}{2}\pi + i\sin\frac{3}{2}\pi) = -32i. \qquad \square$$

$\mathrm{Arg}\,(z^n) = n\ \mathrm{Arg}\ z$ であるから，関数 $f(z) = z^n$ は複素数 z を原点のまわりに回転させることに注意しよう．第 8 章において，この考察に基づいた代数学の基本定理の証明を与える．

$n \in \mathbb{N}, z \in \mathbb{C}$ とする．$w^n = z$ のとき，w は **z の n 乗根**といい，$z^{\frac{1}{n}}$ で表す．$r \in \mathbb{R}$ $(r > 0)$ のとき，r のただ 1 つの実数の n 乗根がある．$z = re^{i\theta}$ とするとき，$w = r^{\frac{1}{n}} e^{i\frac{\theta}{n}}$ は $w^n = z$ を満足し，これは z の 1 つの n 乗根である．しかし，$\dfrac{\theta + 2\pi k}{n} < 2\pi$ $(k \in \mathbb{N})$ であれば，$w_k = r^{\frac{1}{n}} e^{i\frac{\theta+2\pi k}{n}}$ も z の n 乗根の 1 つであり，w とは異なっている．z の異なった n 乗根を与える k の値は $k = 0, 1, \ldots, n-1$ であり，ちょうど n 個である．そのとき，z の n 個の異なった n 乗根は次のようである．

$$w_k = r^{\frac{1}{n}} e^{i\frac{\theta+2\pi k}{n}}, \quad k = 0, 1, \ldots, n-1$$

以上によって，**根に対するド・モアブルの定理**として知られている次の定理を証明したことになる．

根に対するド・モアブルの定理

0 でない複素数 z の異なった n 乗根はちょうど n 個存在する．$z = re^{i\theta}$ と表せば，それらは

$$w_k = r^{\frac{1}{n}} e^{i\frac{\theta+2\pi k}{n}}, \quad k = 0, 1, \ldots, n-1$$

によって与えられる．

例 2.5.2 $z = 1 + i$ として，z の 6 乗根を求めてみよう．

今，$|z| = \sqrt{2}$ であり，$\operatorname{Arg} z = \arctan 1 = \pi/4$ であるから，$z = \sqrt{2}e^{i\frac{\pi}{4}}$．そのとき，$z$ のすべての 6 乗根は次のようである．

(1) $w_1 = r^{\frac{1}{12}} e^{i\frac{\pi/4}{6}} = 2^{\frac{1}{12}}(\cos\frac{\pi}{24} + i\sin\frac{\pi}{24})$.

(2) $w_2 = r^{\frac{1}{12}} e^{i\frac{\pi/4+2\pi}{6}} = 2^{\frac{1}{12}}(\cos\frac{9}{24}\pi + i\sin\frac{9}{24}\pi)$.

(3) $w_3 = r^{\frac{1}{12}} e^{i\frac{\pi/4+4\pi}{6}} = 2^{\frac{1}{12}}(\cos\frac{17}{24}\pi + i\sin\frac{17}{24}\pi)$.

(4) $w_4 = r^{\frac{1}{12}} e^{i\frac{\pi/4+6\pi}{6}} = 2^{\frac{1}{12}}(\cos\frac{25}{24}\pi + i\sin\frac{25}{24}\pi)$.

(5) $w_5 = r^{\frac{1}{12}} e^{i\frac{\pi/4+8\pi}{6}} = 2^{\frac{1}{12}}(\cos\frac{33}{24}\pi + i\sin\frac{33}{24}\pi)$.

(6) $w_6 = r^{\frac{1}{12}} e^{i\frac{\pi/4+10\pi}{6}} = 2^{\frac{1}{12}}(\cos\frac{41}{24}\pi + i\sin\frac{41}{24}\pi)$. □

$|z| = 1$ であるとき，n 乗根 w を **1 の n 乗根**という．$|z| = 1$ であるから，1 の任意の n 乗根 w に対して，$|w| = 1$ である．したがって，1 の n 乗根はそれらの角度だけが異なっている．

系 2.5.1 1 の n 個の異なった n 乗根はすべて次の式で与えられる．

$$w_k = e^{i\frac{2\pi k}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1.$$

幾何学的には，そのとき，1 の n 乗根はすべて半径が 1 の円の上にあり，正の実軸上に 1 つの頂点をもつ内接正 n 角形の頂点に位置している．図 2.5 において，1 の 6 乗根が正 6 角形の頂点をつくっている 6 個の点を描いた．

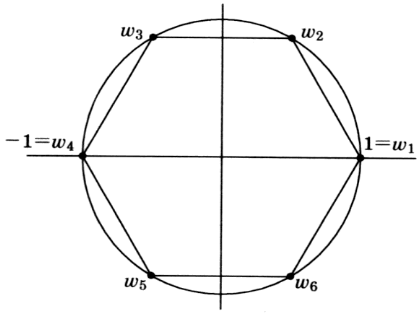


図 2.5　1 の 6 乗根

$|z| \neq 1$ なる 0 でない複素数 z について，n 乗根は半径が $|z|^{\frac{1}{n}}$ の円上の正 n 角形の頂点に位置している．

$w = e^{\boldsymbol{i}\frac{2\pi}{n}}$ を正の最小の角度である 1 の n 乗根とする．これを **1 の主原始 $\boldsymbol{n}$ 乗根**と呼ぶ．他の n 乗根は w の異なったベキである．すなわち，$\{w, w^2, w^3, \ldots, w^n = 1\}$. さらに，これら 1 の n 乗根は乗法に関して群をつくる (w だけが 1 の原始 n 乗根ではないことに注意せよ— 演習問題参照).

系 2.5.2　1 の n 乗根は乗法に関して位数 n の巡回群をつくる．この群は，正の最小の角度をもつ 1 の n 乗根 w によって生成される．

$\boldsymbol{i}$ は 1 の主原始 n 乗根であるから，$\boldsymbol{i}$ のベキに関して前に見た結果はまさにこの系の特別な場合であることがわかる (補題 2.4.1).

演習問題

2.1　$\mathbb{Q}(\sqrt{2})$ は体であることを示せ．

2.2　$\mathbb{Z}_{13}$ において，方程式 $3x + 7 = 6$ を解け (ヒント：$\mathbb{Z}_{13}$ での値を求めよ).

2.3　$\mathbb{Z}_n$ が体であるための必要十分条件は n が素数であることを証明せよ．

2.4　有理数 d が完全平方でなければ，$\mathbb{Q}(\sqrt{d})$ は $\mathbb{R}$ の部分体であることを示せ (d が完全平方であれば，$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$).

2.5　$w^3 = 1, w \neq 1$ とする．このとき，$1 + w + w^2 = 1$ であることを示せ ($w^3 - 1 = 0$ を因数分解せよ).

2.6　$w^3 = 1, w \neq 1$ とする．このとき，演習問題 2.5 より $1 + w + w^2 = 1$, すなわち，$w^2 = -1 - w$ である．$\mathbb{Q}(w) = \{a + bw\,;\, a, b \in \mathbb{Q}\}$ とおき，代

数的操作によって $\mathbb{Q}(w)$ 上に演算を定義せよ．このとき，$\mathbb{Q}(w)$ は $\mathbb{C}$ の部分体であることを示せ (ヒント：$w^2 = -1 - w$ を使う). $\mathbb{Q}(w)$ の $\mathbb{Q}$ 上の拡大次数は何か.

2.7　ここの問題は無限に多くの超越数が存在することを示すことである.

(i) $n \in \mathbb{N}$ に対して，$\mathcal{P}_n =$ [次数 n 以下の有理数係数の多項式の全体] とする．このとき，$\mathcal{P}_n$ は可算集合であることを示せ (ヒント：$\mathcal{P}_n$ は $\mathbb{Q}$ に成分をもつ $n+1$ 個の列の集合と考えることができる．集合 A と B が可算であれば，直積集合 $A \times B$ も可算である).

(ii) $n \in \mathbb{N}$ に対して，$\mathcal{Q}_n =$ [$\mathcal{P}_n$ に属する多項式の根の全体] とする．このとき，$\mathcal{Q}_n$ は可算集合であることを示せ (ヒント：次数 n の多項式は高々 n 個の根をもち，可算集合の可算個の和集合は可算集合である).

(iii) $\mathcal{A}$ を $\mathbb{Q}$ 上代数的である数の集合とするとき，$\mathcal{A}$ は可算であることを示せ (ヒント：$\mathcal{A} = \cup_{n=1}^{\infty} \mathcal{Q}_n$).

(iv) $\mathcal{T}$ を $\mathbb{Q}$ 上超越的である数の集合とするとき，$\mathcal{T}$ は非可算であることを示せ (ヒント：$\mathbb{R} = \mathcal{A} \cup \mathcal{T}$. $\mathcal{T}$ を可算であると仮定せよ).

2.8　実数に対する制限完備性は区間縮小法の原理と同値であることを証明せよ.

2.9　$z = 4 + 7\boldsymbol{i}$, $w = 6 - \boldsymbol{i}$ とするとき，次のものを求めよ.

(i) $\overline{z}$, $\overline{w}$, $|z|$, $|w|$.

(ii) $z + w$, zw, z/w.

(iii) $\sqrt{z}$ (解が 2 つ).

(iii) z を極形式で表せ.

(iv) z^5.

(v) Z の方程式 $zZ + 6w = 1 - \boldsymbol{i}$ を解け.

2.10　補題 2.2.1 を証明せよ.

2.11　補題 2.2.2 を証明せよ.

2.12　演習問題 2.9 において，積 $zw = 4w + \boldsymbol{i}7w$ を計算し，w についての幾何学的な操作を追跡せよ.

2.13　演習問題 2.9 において，z と w を極形式になおしてかけ算せよ．計算機によって，Arg z と Arg w を推定せよ.

2.14 $z = 1 + \sqrt{3}i$ とするとき，次を求めよ．

(i) z^{26}.

(ii) z のすべての 5 乗根.

(iii) (ii) に対する答えを図に幾何学的に描け.

2.15 $\{1, w, w^2, \dots, w^{n-1}\}$ が位数 n の巡回群をつくると仮定する．このとき，w^k が G を生成するための必要十分条件は $(k, n) = 1$ であることを示せ (ヒント：$(k, n) = 1$ であれば，k と n は互いに素であり，1 は k と n の 1 次結合で表される).

2.16 $w = e^{2\pi i/8}$ を 1 の主原始 8 乗根とする．w のどのようなベキが，8 乗根がつくる群を生成するか?

第3章

多項式と複素多項式

3.1 体上の多項式環

F を体とし，n を正の整数とする．**F 上の次数 n の多項式**とは次のような形をしている形式的な和のことである．

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{3.1}$$

ただし，$a_i \in F$ $(i = 0, \ldots, n)$, $a_n \neq 0$ で，x は不定元である．F 上の多項式 $P(x)$ はある次数をもつ多項式であるか，または $P(x) = 0$ である．0 は**ゼロ多項式**と呼ばれ，次数をもたない．$P(x)$ の次数を $\mathbf{deg}\, \boldsymbol{P(x)}$ で表す．次数 0 の多項式は $P(x) = a_0$ という形で**定数多項式**といい，F の元と同一視することができる．式 (3.1) に現れる元 $a_i \in F$ は多項式 $P(x)$ の**係数**と呼ばれ，特に a_n を**最高次係数**という．$a_n = 1$ のとき，$P(x)$ は**モニック多項式**という．2 つの 0 でない多項式が等しいとは，それらが同じ次数をもち，同じ係数をもつことである．次数 1 の多項式は **1 次多項式**，次数 2 の多項式は **2 次多項式**という．

F 上のすべての多項式の集合を $F[x]$ で表し，ゼロ多項式と次数 n 以下のすべての多項式の集合を $F_n[x]$ で表す．

$$F[x] = \{P(x)\ ;\ P(x) \text{ は } F \text{ 上の多項式}\}. \tag{3.2}$$

$$F_n[x] = \{P(x) \in F[x]\ ;\ \deg P(x) \leq n \text{ または } P(x) = 0\}. \tag{3.3}$$

後で，$F[x]$ は整数環 $\mathbb{Z}$ とほぼ同じ性質をもつ環になることがわかるであろう．はじめに，$F[x]$ 上に加法，減法，乗法を代数的操作によって定義する．すなわち，$P(x) = a_0 + a_1x + \cdots + a_nx^n$，$Q(x) = b_0 + b_1x + \cdots + a_mx^m$ に対して

$$P(x) \pm Q(x) = (a_0 \pm b_0) + (a_1 \pm b_1)x + \cdots \tag{3.4}$$

とおく．すなわち，$P(x) \pm Q(x)$ における x^i の係数は $a_i \pm b_i$ である．また，

$$P(x)Q(x) = (a_0b_0) + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots + (a_nb_m)x^{n+m} \tag{3.5}$$

すなわち，$P(x)Q(x)$ における x^i の係数は $(a_0b_i + a_1b_{i-1} + \cdots + a_ib_0)$ である．

例 3.1.1　$P(x) = 3x^2 + 4x - 6$, $Q(x) = 2x + 7$ を $\mathbb{Q}[x]$ の多項式とすると

$$P(x) + Q(x) = 3x^2 + 6x + 1$$

であり，

$$P(x)Q(x) = (3x^2 + 4x - 6)(2x + 7) = 6x^3 + 29x^2 + 16x - 42. \qquad \square$$

定義より，次数に関する次の関係は明らかである．証明は演習問題として残す．

補題 3.1.1　$P(x)$ と $Q(x)$ を F 上の多項式とし，$P(x) \neq 0, Q(x) \neq 0$ とする．このとき，次のことが成り立つ．

(1) $\deg P(x)Q(x) = \deg P(x) + \deg Q(x)$.

(2) $\deg(P(x) \pm Q(x)) \leq Max(\deg P(x), \deg Q(x))$.

環 R の元 r が**零因子**であるとは，あるゼロではない元 s が存在して，$rs = 0$ を満たすことである．たとえば 6 を法とする整数環 $\mathbb{Z}_6$ において，2 と 3 はどちらもゼロではない．ところが $(2)(3) = 0$ であるから，2 と 3 はどちらも零因子である．単位元をもつ可換環で，零因子をもたないものを**整域**という．整域の例としては，$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$，そして p を素数として $\mathbb{Z}_p$ がある．次の補題で示すように，一般に体は必然的に整域になる．環において，乗法の逆元をもつ元のことを**単元**と呼んだことを思い起こしておこう．

補題 3.1.2 R を単位元をもつ可換環とする．$r \in R$ が単元であれば，r は零因子ではない．特に，R が体であれば，R は整域である．

（証明） $r \in R$ として，$rs = 0$ と仮定する．r は単元であるから，$r^{-1}r = 1$ を満たす元 $r^{-1} \in R$ が存在する．そのとき，$r^{-1}(rs) = r^{-1}0 = 0$ であるが，一方 $r^{-1}(rs) = (r^{-1}r)s = 1s = s$ である．ゆえに，$s = 0$ となり，r は零因子ではない．

体 F は単位元をもつ可換環であって，すべてのゼロではない元は単元である．上で示したことより，F のゼロでない元は零因子ではない．よって，F は整域である．■

さて，ここで次の定理を証明することができる．

定理 3.1.1 F を体とすれば，$F[x]$ は単位元をもつ可換環である（実際には整域である）．F の各元を対応している $F[x]$ の定数多項式と同一視することによって，F を $F[x]$ の中に自然に埋め込むことができる．$F[x]$ の単元は，F のゼロでない元のみである．$F_n[x]$ は F 上に $n+1$ 次元のベクトル空間をつくる．

（証明） 基本的な環論的性質を確かめるのは単なる計算なので，演習問題に委ねてある．$\deg P(x)Q(x) = \deg P(x) + \deg Q(x)$ であるから，$P(x) \neq 0, Q(x) \neq 0$ とすれば，$P(x)Q(x) \neq 0$ である．したがって，$F[x]$ は整域である．

$G(x)$ が $F[x]$ において単元とすると，ある $H(x) \in F[x]$ が存在して $G(x)H(x) = 1$ を満たす．次数を比較すると，$\deg G(x) + \deg H(x) = 0$. ところが，$\deg G(x) \geq 0, \deg H(x) \geq 0$ であるから，これは $\deg G(x) = \deg H(x) = 0$ のときだけ可能である．したがって，$G(x) \in F$ となる．

最後に，補題 3.1.1 より $F_n[x]$ は加法と減法に関して閉じている．ゆえに，$F_n[x]$ はアーベル群である．F の元をかけるという乗法は次数を上げないので，$F_n[x]$ にスカラー乗法を定義する．したがって，$F_n[x]$ は F 上のベクトル空間をつくる．集合 $\{1, x, x^2, \ldots, x^n\}$ は基底をつくり，$\dim(F_n[x]) = n+1$ となる．■

多項式 $P(x) \in F[x]$ は**代入**によって関数 $P : F \longrightarrow F$ と考えることができ

る．$P(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ とする．F は多項式の表現の中で使われるすべての演算に関して閉じているので，$t \in F$ に対して

$$P(t) = a_0 + a_1t + \cdots + a_nt^n \in F.$$

体 F がある意味で——コーシー完備性のような意味で——閉じていれば，この関数は連続である．特に，実多項式そして複素多項式はそれぞれ連続関数 $\mathbb{R} \longrightarrow \mathbb{R}, \mathbb{C} \longrightarrow \mathbb{C}$ と考えることができる．

$r \in F, P(x) \in F[x]$ とする．代入して $P(r) = 0$ のとき，r は $P(x)$ の**根**または $P(x)$ の**ゼロ**という．また同じ意味で，$\boldsymbol{r}$ **は** $\boldsymbol{P(x)}$ **を満足する**という．序文のところで指摘したように，多くの著者は方程式に対して根という言葉を使い，多項式と関数に対してゼロという言葉を用いる傾向がある．この本を通して，我々は根のほうを使うことにする．歴史的には根という言葉は非常に頻繁に代数学の基本定理と関連して用いられてきたのである．次の章において，r が根であることは因数分解の可能性を意味しているということがわかるであろう．

3.2　整除と多項式の一意分解性

体 F に対して，多項式環 $F[x]$ の代数的構造は整数環 $\mathbb{Z}$ のそれに驚くほど類似している．$\mathbb{Z}$ は次に述べるような**算術の基本定理**と呼ばれている基本的な性質を満足していることを思い起こそう．

算術の基本定理

$z \in \mathbb{Z}$ を整数とすると，z は素数の積に分解される．さらに，この分解は積の順序と単元を除いて一意的である．

一般に，素数の積に一意的に分解される（順序と単元を除いて）整域は**一意分解整域**と呼ばれ，簡約記号で **UFD** と表される．この定義によれば，算術の基本定理は，$\mathbb{Z}$ が UFD であることを意味していることになる．さて，任意の体 F に対して，多項式環 $F[x]$ が UFD であることを示そう．まず最初に，因数分解と素数を定義しなければならない．

定義 3.2.1　$f(x), g(x) \in F[x], g(x) \neq 0$ とする．ある多項式 $q(x) \in F[x]$ が存

在して，$f(x) = q(x)g(x)$ を満たすとき，$g(x)$ は $f(x)$ を**割り切る**，または，$g(x)$ は $f(x)$ の**因数**であるという．これを，$g(x) \mid f(x)$ によって表す．

0 でない多項式 $f(x)$ が，自明でなくかつ単元でない因数をもたない（低い次数の多項式に分解できない）とき，$f(x)$ は**既約多項式**という．明らかに，$\deg g(x) = 1$ であれば，$g(x)$ は既約多項式である．

多項式環 $F[x]$ が UFD であることは，整数に対する除法の定理とまったくの類似である多項式に対する除法の定理より従う．

$F[x]$ における除法の定理　$F[x]$ の 0 でない多項式 $f(x), g(x)$ に対して，$f(x) = q(x)g(x) + r(x)$，$r(x) = 0$ または $\deg r(x) < \deg g(x)$ を満たすただ 1 つの多項式 $q(x)$ と $r(x)$ が存在する (多項式 $q(x)$ と $r(x)$ はそれぞれ商と剰余という).

この定理の証明は本質的には多項式の割算の繰返しである．形式的な証明は $\deg g(x)$ の次数に関する帰納法に基づいている．証明は省略し，$\mathbb{Q}[x]$ における例をあげよう．

例 3.2.1

(a) $f(x) = 3x^4 - 6x^2 + 8x - 6$，$g(x) = 2x^2 + 4$ とするとき，

$$\frac{3x^4 - 6x^2 + 8x - 6}{2x^2 + 4} = \frac{3}{2}x^2 - 6 \quad 余り \quad 8x + 18.$$

このとき，$q(x) = \frac{3}{2}x^2 - 6$，$r(x) = 8x + 18$.

(b) $f(x) = 2x^5 + 2x^4 + 6x^3 + 10x^2 + 4x$，$g(x) = x^2 + x$ とするとき，

$$\frac{2x^5 + 2x^4 + 6x^3 + 10x^2 + 4x}{x^2 + x} = 2x^3 + 6x + 4.$$

このとき，$q(x) = 2x^3 + 6x + 4$，$r(x) = 0$. □

除法の定理を使って，$\mathbb{Z}$ におけるように $F[x]$ の 一意分解性が得られる．このためには，**最大公約数 (gcd)** の概念と，以下に示す 2 つの補題が必要である．

定義 3.2.2

(1) $f(x), g(x) \in F[x]$ とする．$d(x) \in F[x]$ が次の条件を満たすとき，$d(x)$ を $f(x)$ と $g(x)$ の**最大公約数**または **gcd** という．

(i) $d(x) \in F[x]$ がモニックであり，

(ii) $d(x)$ は $f(x)$ と $g(x)$ を割り切り，かつ

(iii) $d_1(x) \in F[x]$ が $f(x)$ と $g(x)$ を割り切るとき，$d(x)$ が $d_1(x)$ を割り切る．

このとき，$d(x) = (g(x), f(x))$ と書く．$(f(x), g(x)) = 1$ のとき，$f(x)$ と $g(x)$ は**互いに素**であるという．

(2) $f(x)h(x) + g(x)k(x)$ という式の表現を $f(x)$ と $g(x)$ の **1 次結合**という．

補題 3.2.1 $f(x), g(x) \in F[x]$ とする．このとき，$f(x)$ と $g(x)$ の最大公約数はただ 1 つ存在する．それは $f(x)$ と $g(x)$ の 1 次結合で表されているものの中で最小の次数をもつモニックな多項式である．

2 つの多項式の最大公約数を求めることは，2 つの整数の最大公約数を求めるのと同じ方法でなされる．すなわち，**ユークリッドの互除法**を使って，次のようになされる．$0 \neq f(x), 0 \neq g(x) \in F[x]$ とする．除法の定理を繰り返し使うことによって，次の一連の式を得る．

$$\begin{aligned} f(x) &= q(x)g(x) + r(x), \\ g(x) &= q_1(x)r(x) + r_1(x), \\ r(x) &= q_2(x)r_1(x) + r_2(x), \\ &\cdots \\ &\cdots \\ r_{k-1}(x) &= q_{k+1}(x)r_k(x). \end{aligned}$$

各式の割算は次数を下げ，その次数は有限であるから，その操作は有限回で終わる．$r_k(x)$ をその最後のゼロでない剰余である多項式とし，c を $r_k(x)$ の最高次係数とする．このとき，$c^{-1}r_k(x)$ が求める最大公約数である．例を与えよう．

例 3.2.2 $\mathbb{Q}[x]$ において，$f(x) = x^3 - 1$ と $g(x) = x^2 - 2x + 1$ の最大公約数を求め，それを $f(x)$ と $g(x)$ の 1 次結合で表せ．

ユークリッドの互除法を使えば,

$$x^3 - 1 = (x^2 - 2x + 1)(x + 2) + (3x - 3),$$
$$x^2 - 2x + 1 = (3x - 3)(\frac{1}{3}x - \frac{1}{3}).$$

したがって,最後のゼロでない剰余は $3x - 3$ である.ゆえに,それらの最大公約数は $x - 1$ である.はじめの式に戻ると,

$$3x - 3 = (x^3 - 1) - (x^2 - 2x + 1)(x + 2).$$

したがって,

$$x - 1 = \frac{1}{3}(x^3 - 1) - \frac{1}{3}(x^2 - 2x + 1)(x + 2).$$

これは求めた最大公約数が,はじめに与えられた 2 つの多項式の 1 次結合であることを表している. □

補題 3.2.2 (ユークリッドの補題) $p(x)$ を既約多項式とする.$p(x)$ が $f(x)g(x)$ を割り切るとき,$p(x)$ は $f(x)$ を割り切るかまたは $g(x)$ を割り切る.

(証明) $p(x)$ が $f(x)$ を割り切らないと仮定する.そのとき,$p(x)$ は既約であるから,$p(x)$ と $f(x)$ は互いに素でなければばらない.したがって,ある多項式 $h(x), k(x)$ があって,次が成り立つ.

$$f(x)h(x) + p(x)k(x) = 1.$$

両辺に $g(x)$ をかけると,次を得る.

$$g(x)f(x)h(x) + g(x)p(x)k(x) = g(x).$$

今,$p(x) \mid g(x)f(x)$ であるから,$p(x)$ は左辺の各項を割り切るので,$p(x) \mid g(x)$ を得る. ■

例 3.2.3 $x^2 + x + 1$ は $\mathbb{Q}[x]$ と $\mathbb{R}[x]$ において既約であるが,$\mathbb{C}[x]$ においては既約でないことを示せ.

$f(x) = x^2+x+1$ が $\mathbb{R}[x]$ で自明でない因数をもったと仮定する.$\deg f(x) = 2$ であり,この因数の次数は 1 でなければならないから,$f(x)$ は 2 つの因数の積に分解する.

$$f(x) = x^2 + x + 1 = (ax + b)(cx + d).$$

それで，$f(x)$ は実根をもつ，すなわち，$-b/a$ である．しかし，2 次方程式の根の公式より，その根は次のようになる．

$$\omega_1 = \frac{-1+\sqrt{3}i}{2}, \quad \omega_2 = \frac{-1-\sqrt{3}i}{2}.$$

これらの根はいずれも実数ではない．したがって，$f(x)$ は $\mathbb{R}[x]$ 上で既約でなければならない，当然 $\mathbb{Q}[x]$ においても既約である．

$\mathbb{C}[x]$ における計算によって，$f(x) = (x-\omega_1)(x-\omega_2)$ であることがわかる．したがって，$f(x)$ は $\mathbb{C}[x]$ で分解する．□

定理 3.2.1 $F[x]$ の 0 でない多項式 $f(x)$ は既約多項式の積に分解する．この分解は順序と単元を除いて一意的である．すなわち，$F[x]$ は一意分解整域 (UFD) である．

証明は整数環 $\mathbb{Z}$ に対する証明とほとんど同じである．簡単にそれをスケッチしてみよう．はじめに，既約分解を得るために $f(x)$ の次数に関する帰納法を使う．$\deg f(x) = 1$ のとき，$f(x)$ は既約であるから，$\deg f(x) = n > 1$ と仮定する．$f(x)$ が既約であれば，それは 1 つの既約分解をもつ．$f(x)$ が既約でなければ，$f(x) = g(x)h(x)$, $\deg g(x) < n, \deg h(x) < n$ と分解される．帰納法の仮定によって，$g(x)$ と $h(x)$ は既約分解をもつので，$f(x)$ も同様に既約分解をもつことになる．

さて，次に $f(x)$ は 2 つの既約分解をもったと仮定しよう．

$$f(x) = p_1(x)^{n_1} \cdots p_k(x)^{n_k} = q_1(x)^{m_1} \cdots q_t(x)^{m_t},$$

ここで，$p_i(x)$, $i = 1, \ldots, n$, $q_j(x)$, $j = 1, \ldots, t$ は既約多項式である．このとき，$p_i(x) \mid q_1(x)^{m_1} \cdots q_t(x)^{m_t}$ であるから，ユークリッドの補題よりある j に対して $p_i(x) \mid q_j(x)$ である．2 つとも既約であるからある単元 c があって $p_i(x) = cq_j(x)$ となっている．これを繰り返し適用すれば $n_i = m_j$ を得る．以上より，単元を除いて同じ既約因数，同じ重複度をもつことがわかる．したがって，定理が証明された．

この証明の推論は体 F でなくて，可換環 R であっても可能である．R が UFD であれば，$R[x]$ も UFD であることが証明できる．このようにして，$\mathbb{Z}[x]$ も UFD である．その証明は体の場合のそれとは異なっており，もう少し複雑である．

3.3 多項式の根と因数分解

$P(x)$ を次数が 1 より大きい体 F 上の多項式とする．$P(x)$ が F に根をもつならば，$P(x)$ は $F[x]$ で分解すること，すなわち，$P(x)$ は既約多項式ではないことを証明する．

補題 3.3.1 $c \in F$ が $P(x)$ の根ならば，$(x-c)$ は $P(x)$ を割り切る．すなわち，$P(x) = (x-c)Q(x)$ が成り立つ．ここで，$\deg Q(x) = \deg P(x) - 1$ である．

（証明） $P(c) = 0$ と仮定する．除法の定理より，$P(x) = (x-c)Q(x) + r(x)$ と表される．ここで，$\deg r(x) < \deg(x-c) = 1$ であるから，$r(x) = 0$ であるかまたは $r(x) = a \in F$ である．ゆえに，

$$P(x) = (x-c)Q(x) + a.$$

c を代入すると，$P(c) = 0 + a = 0$ であるから，$a = 0$ となる．したがって，$P(x) = (x-c)Q(x)$ を得る． ■

系 3.3.1 体 F 上の 1 より大きい次数の既約多項式は F に根をもたない．

この補題 3.3.1 より次の重要な定理が得られる．

定理 3.3.1 $F[x]$ に属する次数 n の多項式は高々 n 個の根をもつ．

（証明） $P(x)$ の次数を n とし，n についての帰納法で示す．$n = 1$ のとき，$P(x)$ は $P(x) = ax + b$ $(a, b \in F, a \neq 0)$ と表される．このとき，$P(x)$ はただ 1 つの根 $-b/a \in F$ をもつ．

$n > 1$ として，$n-1$ までは定理が成り立つと仮定し，n のときに成り立つことを証明する．$c_1 \in F, P(c_1) = 0$ と仮定する．このとき補題 3.3.1 により，

$$P(x) = (x - c_1)Q(x)$$

を満たす多項式 $Q(x) \in F[x]$ がある．帰納法の仮定より $Q(x)$ は高々 $n-1$ 個の根をもつので，$P(x)$ の根は高々 n 個である． ■

次数 n の多項式は最大 n 個の根をもち，それらの根は一意的である．なぜならば，$P(x)$ の次数を n とし，それらの根を $c_1, \ldots, c_k$ $(k \leq n, c_i \in F)$ とする．そのとき，$F[x]$ における一意分解性によって

$$P(x) = (x - c_1)^{m_1} \cdots (x - c_k)^{m_k} Q_1(x) \cdots Q_t(x)$$

と表される．ここで，$Q_i(x)$, $i = 1, \ldots, t$ はすべて定数であるか，または次数が 1 より大きい既約多項式である．指数 m_i は根 c_i の**重複度**と呼ばれる．$c \in F$ を $P(x)$ の 1 つの根とする．このとき，

$$(c - c_1)^{m_1} \cdots (c - c_k)^{m_k} Q_1(c) \cdots Q_t(c) = 0.$$

$Q_i(x)$ は定数であるか，または次数が 1 より大きい既約多項式であるから，$Q_i(c) \neq 0$ $(i = 1, \cdots, t)$ である．したがって，ある i に対して $(c - c_i) = 0$. ゆえに，$c = c_i$ となる．

系 3.3.2 $P(x)$ を次数 2 または 3 の多項式とする．このとき，$P(x)$ が既約であるための必要十分条件は，$P(x)$ が F に根をもたないことである．

（証明） $P(x)$ が既約であると仮定する．$\deg P(x) > 1$ であるから，$P(x)$ は F に根をもたない．逆に，$P(x)$ が F に根をもたないと仮定する．もし，$P(x)$ が既約でなかったとすると，それは 2 つの次因数に分解され，1 つは 1 次式である．

$$P(x) = (ax + b)g(x),\ g(x) \in F[x].$$

ところが，そのとき $P(x)$ は根 $-b/a \in F$ をもつ．これは矛盾である．■

3.4　実多項式と複素多項式

ここで基礎となる体を実数体 $\mathbb{R}$ あるいは複素数体 $\mathbb{C}$ を考え，実多項式と複素多項式，すなわち，それぞれ，$\mathbb{R}[x]$ と $\mathbb{C}[x]$ に属する多項式を考える．はじめに，次の重要な結果が必要である．

定理 3.4.1 奇数次の実多項式は実根をもつ．

（証明） $P(x) \in \mathbb{R}[x]$, $\deg P(x) = n = 2k+1$ とし，最高次係数を $a_n > 0$ と仮定する ($a_n < 0$ の場合でも証明はほとんど同じである)．そのとき，

$$P(x) = a_n x^n + (\text{低い次数の項}),\ n \text{ は奇数}$$

と表される．すると，

(1) $\displaystyle\lim_{x\to\infty} P(x) = \lim_{x\to\infty} a_n x^n = \infty$ ($a_n > 0$ であるから).
(2) $\displaystyle\lim_{x\to-\infty} P(x) = \lim_{x\to-\infty} a_n x^n = -\infty$ ($a_n > 0$ かつ n は奇数であるから).

(1) より，$P(x)$ はいくらでも大きな正の数の値をとることができるので，ある実数 x_1 があって $P(x_1) > 0$ を満たす．同様に，(2) よりある実数 x_2 があって $P(x_2) < 0$ を満たす．

実多項式はすべての $x \in \mathbb{R}$ に対して，連続な実数値関数である．$P(x_1)P(x_2) < 0$ であるから，中間値の定理より x_1 と x_2 の間にある x_3 が存在して $P(x_3) = 0$ が成り立つ． ■

この定理の直接的な結果として次の系が成り立つ．

系 3.4.1 $P(x) \in \mathbb{R}[x]$ が既約で，1 次式でなければその次数は偶数である (後で，その次数は 2 であることがわかる)．

さて，次に複素多項式を考察する．

補題 3.4.1 すべての次数 2 の複素多項式は $\mathbb{C}$ に根をもつ．

（証明） これは，まさに 2 次方程式の根の公式である．$P(x) = ax^2 + bx + c$ とおけば，それらの根は形式的に次のように与えられる．

$$x_1 = \frac{-b + \sqrt{b^2 - 4ab}}{2a}, \quad x_2 = \frac{-b - \sqrt{b^2 - 4ab}}{2a}.$$

ド・モアブルの定理より，すべての複素数は平方根をもつ．ゆえに，x_1, x_2 は $\mathbb{C}$ の中に存在する．もちろん，それらは $b^2 - 4ac = 0$ であれば同じである． ■

さらに議論を進めるために，**多項式の共役**という概念とこの概念からただちに得られるいくつかの補題について述べよう．

定義 3.4.1 $P(x) = a_0 + a_1x + \cdots + a_nx^n$ を複素多項式とするとき，その共役を $\overline{P}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$ によって定義する．すなわち，$P(x)$ の共役とはその係数が $P(x)$ の係数の共役である多項式のことである．

補題 3.4.2 任意の複素多項式 $P(x) \in \mathbb{C}[x]$ に対して次が成り立つ．

(1) $\overline{P(z)} = \overline{P}(\bar{z}) \quad (z \in \mathbb{C})$.

(2) $P(x)$ が実多項式であるための必要十分条件は $P(x) = \overline{P}(x)$.

(3) $H(x) = P(x)Q(x)$ ならば $\overline{H}(x) = \overline{P}(x)\overline{Q}(x)$.

（証明） (1) $z \in \mathbb{C}$, $P(z) = a_0 + \cdots + a_nz^n$ とする．このとき，

$$\overline{P(z)} = \overline{a_0 + \cdots + a_nz^n} = \bar{a}_0 + \bar{a}_1\bar{z} + \cdots + \bar{a}_n\bar{z}^n = \overline{P}(\bar{z}).$$

(2) $P(x)$ を実多項式と仮定すると，そのすべての係数に対して $a_i = \bar{a}_i$ であるから，$P(x) = \overline{P}(x)$. 逆に，$P(x) = \overline{P}(x)$ と仮定する．そのとき，そのすべての係数に対して $a_i = \bar{a}_i$ であるから，$a_i \in \mathbb{R}$. したがって，$P(x)$ は実多項式である．

(3) 証明は単なる計算であるから，演習問題として残しておく． ■

補題 3.4.3 $G(x) \in \mathbb{C}[x]$ ならば，$H(x) = G(x)\overline{G}(x) \in \mathbb{R}[x]$.

（証明） $\overline{H}(x) = \overline{G(x)\overline{G}(x)} = \overline{G}(x)\overline{\overline{G}}(x) = \overline{G}(x)G(x) = G(x)\overline{G}(x) = H(x)$. ゆえに，$H(x)$ は実多項式である． ■

補題 3.4.4 $f(x) \in \mathbb{R}[x]$ とする．$f(z_0) = 0$ ならば，$f(\bar{z}_0) = 0$. すなわち，実多項式の複素数の根はその共役と対で根となっている．

（証明） $f(z_0) = 0$ ならば $\overline{f(z_0)} = 0$. ところがそのとき，$\bar{f}(\bar{z}_0) = 0$ である．$f(x)$ は実多項式であるから，$f(x) = \bar{f}(x)$. ゆえに，$f(\bar{z}_0) = 0$. ■

z_0 が $f(x) \in \mathbb{R}[x]$ の根であれば，$(x - z_0)$ と $(x - \bar{z}_0)$ は 2 つとも $f(x)$ を割り切ることに注意しよう．

補題 3.4.5 任意の複素数 $z \in \mathbb{C}$ に対して，$(x - z)(x - \bar{z}) \in \mathbb{R}[x]$ が成り立つ．

この証明は演習問題とする．この補題によって次数 3 以下の任意の実多項式は複素数体 $\mathbb{C}$ の範囲では完全に 1 次因数に分解することがわかる．

最後にこの節を終えるにあたり，次の定理を証明する．この定理は，代数学の基本定理を証明するためには，すべての定数でない実多項式が複素数の根をもつ，ということを証明しさえすればよいことを示している．

定理 3.4.2 すべての定数でない実多項式が少なくとも 1 つの複素数の根をもてば，すべての定数でない複素多項式が少なくとも 1 つの複素数の根をもつ．

（**証明**）$P(x) \in \mathbb{C}[x]$ として，すべての定数でない実多項式が少なくとも 1 つの複素数の根をもつと仮定する．$H(x) = P(x)\overline{P}(x)$ とおく．補題 3.4.3 によって，$H(x) \in \mathbb{R}[x]$. 仮定によって，ある $z_0 \in \mathbb{C}$ が存在して $H(z_0) = 0$. そのとき，$P(z_0)\overline{P}(z_0) = 0$. $\mathbb{C}$ は零因子をもたないから，$P(z_0) = 0$ であるかまたは $\overline{P}(z_0) = 0$ である．前者の場合 z_0 が $P(x)$ の根である．後者の場合 $\overline{P}(z_0) = 0$ であるが，そのとき補題 3.4.2 より，$0 = \overline{P}(z_0) = \overline{\overline{P}}(\bar{z}_0) = P(\bar{z}_0)$ である．したがって，$\bar{z}_0$ は $P(x)$ の根である． ■

この定理は代数学の基本定理ではない．これは単に，代数学の基本定理を証明するためには，実多項式に対してのみそれを示せばよいことを言っているだけである．

3.5 代数学の基本定理——証明 1

ここで，代数学の基本定理の第 1 の証明を与えよう．この証明は高等微積分学にのみ基づいており，高等微積分学から次の結果を必要とする．

補題 3.5.1 D を $\mathbb{R}^2$ の有界閉集合（コンパクト）とする．$f : D \longrightarrow \mathbb{R}$ が連続であれば，$f(x, y)$ は D において最大値と最小値をとる．

これは初等微積分学における**最大値・最小値の定理**の 2 次元版である．最大値・最小値の定理とは，$f : [a, b] \longrightarrow \mathbb{R}$ が連続関数であれば，$f(x)$ は $[a, b]$ の上で最小値，最大値をとるというものである．この定理は，より一般的に $n \geq 1$ としたとき，コンパクトな領域上で 連続関数 $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ に対して成り立つ．補題 3.5.1 の証明については，適当な高等微積分学の本を参照していただきたい．

定理 3.5.1（代数学の基本定理）$f(x)$ を定数でない複素多項式とすれば，$f(x)$ は少なくとも 1 つ複素数の根をもつ．

証明は次の 2 つの補題によって与えられる．

補題 3.5.2 $f(x) \in \mathbb{C}[x]$ とする．$|f(x)|$ はある点 $z_0 \in \mathbb{C}$ において最小値をとる．

（証明） $|x| \to \infty$ ならば, $|f(x)| \to \infty$ であることはただちにわかる．大きな $|x|$ に対して，$|f(x)|$ は大きいから，$z \in \mathbb{C}$ に対する $|f(z)|$ の下限はある十分大きな円板 $|z| \leq r$ における下限でもある．

$|f(x)|$ は連続な実数値関数であるから，補題 3.5.1 より $|f(x)|$ はこの円板上でその最小値をとる．■

補題 3.5.3 $f(x) \in \mathbb{C}[x]$ でかつ $f(x)$ は定数ではないと仮定する．$f(x_0) \neq 0$ ならば，$|f(x_0)|$ は $|f(x)|$ の最小値ではない．

（証明） $f(x)$ は定数でない複素多項式とし，x_0 は $f(x_0) \neq 0$ を満たしている点とする．x を $x + x_0$ と変数変換する．これが，x_0 を原点に移すとして，以下 $f(0) \neq 0$ と仮定することができる．次に，$f(x)$ に $f(0)^{-1}$ をかけると，$f(0) = 1$ となる．そのとき，1 が $|f(x)|$ の最小値ではないことを示さなければならない．

k を多項式 $f(x)$ に現れる 0 でない項の x の最小のベキ指数とする．そのとき， $f(x)$ は次のような形で表される．

$$f(x) = 1 + ax^k + (k \text{ より大きい次数の項}).$$

今，$-a^{-1}$ の k 乗根の 1 つを α とする．これは，ド・モアブルの定理により存在する．変数 x を αx とする最後の変換をする．すると，$f(x)$ は適当な $g(x) \in \mathbb{C}[x]$ によって，

$$f(x) = 1 - x^k + x^{k+1}g(x)$$

と表される．非常に小さい正の実数 x に対して三角不等式より，次の式を得る．

$$|f(x)| \leq |1 - x^k| + x^{k+1}|g(x)|.$$

しかし，非常に小さい実数 x に対して $x^k < 1$ であるから，上式は次の形になる．

$$|f(x)| \leq 1 - x^k + x^{k+1}|g(x)| = 1 - x^k(1 - x|g(x)|).$$

非常に小さい実数 x に対して，$x|g(x)|$ も小さいので，x_0 を $x_0|g(x_0)| < 1$ であるように選ぶことができる．したがって，$x_0^k(1 - x_0|g(x_0)|) > 0$. ゆえに，$|f(x_0)| < 1 = |f(0)|$ となる．これより補題は証明された． ■

これら 2 つの補題を組み合わせれば，代数学の基本定理の第一の証明を得る．

（証明） $f(x)$ をゼロでない複素多項式とする．補題 3.5.2 より，$|f(x)|$ はある点 $x_0 \in \mathbb{C}$ において最小値をとる．そのとき，補題 3.5.3 より，$|f(x_0)| = 0$. ゆえに，$f(x_0) = 0$. なぜなら，そうでなければ $f(x_0)$ は最小値ではないからである．したがって，$f(x)$ は複素数の根をもつ． ■

3.6 代数学の基本定理の結果

この章の最後に，代数学の基本定理から得られるいくつかの結果を見てみよう．

系 3.6.1 複素多項式は完全に 1 次因数に分解する．

（証明） $f(x)$ として，その次数についての帰納法を用いる．$\deg f(x) = 1$ のときは，$f(x)$ はそれ自身 1 次式であるから，この系は成り立つ．$\deg f(x) = n$ と仮定する．代数学の基本定理より，1 つの根 x_0 が存在する．したがって，$x - x_0$ は $f(x)$ を割り切る．ゆえに，ある多項式 $g(x) \in \mathbb{C}[x]$ があって $f(x) = (x - x_0)g(x)$ と表される．ここで，$\deg g(x) < n$ である．帰納法の仮定より，$g(x)$ は 1 次因数に分解する．それゆえ，$f(x)$ も 1 次因数に分解する． ■

系 3.6.2 $f(x) \in \mathbb{C}[x]$, $\deg f(x) = n$ とし，$f(x)$ の根を $x_1, x_2, \ldots, x_n$ とする（重複も可とする）．そのとき，$f(x)$ は次のように表される．

$$f(x) = \alpha(x - x_1)(x - x_2)\cdots(x - x_n), \quad \alpha \in \mathbb{C}.$$

系 3.6.3 実多項式は $\mathbb{R}[x]$ において次数 1 と次数 2 の多項式に分解する．すなわち，既約な実多項式は 1 次多項式と実根をもたない 2 次多項式だけである．

（証明） $f(x) \in \mathbb{R}[x]$ と仮定すれば，当然 $f(x) \in \mathbb{C}[x]$ である．$z_1, z_2, \ldots, z_n$ をその複素数の根とすると，

$$f(x) = \alpha(x - z_1)(x - z_2)\cdots(x - z_n).$$

ここで，α は $f(x)$ の最高次係数であるから，$\alpha \in \mathbb{R}$ である．

z_i が実数であれば，$(x - z_i)$ は実数係数の 1 次因数である．$z_i \notin \mathbb{R}$ ならば，その複素共役 $\bar{z}_i$ も $f(x)$ の根である．ところがそのとき，$(x - z_i)(x - \bar{z}_i)$ は次数 2 の実多項式の因数である． ■

系 3.6.4 既約な実多項式の次数は 1 か 2 である．

ここで呈示した代数学の基本定理の証明は，より一般的なリウヴィルの定理に基づく第 2 の証明へと導く動機となる．リウヴィルの定理によれば，複素平面において有界である整関数は定数でなければならない．整関数とは $\mathbb{C}$ の各点において，複素数の微分係数をもつ複素関数である．この定理を理解するためには，複素解析学，すなわち，複素関数に対する解析学を少し学ばねばならない．このことを，次の 2 つの章で行う．

演習問題

3.1　補題 3.1.1 を証明せよ．すなわち，$P(x), Q(x) \in F[x]$ とするとき，$\deg P(x)Q(x) = \deg P(x) + \deg Q(x), \deg(P(x) \pm Q(x)) \leq \mathrm{Max}(\deg P(x), \deg Q(x))$ が成り立つことを示せ．

3.2　環の定義が成り立つことを示すことによって，$F[x]$ が可換環であることを確かめよ．

3.3　S を体 F の部分環とせよ（$\mathbb{R}$ における $\mathbb{Z}$ のように）．$S[x]$ を S に係数をもつ $F[x]$ の多項式の全体とする．$S[x]$ は $F[x]$ の部分環であることを示せ．ある部分集合が部分環であることを示すにはそれが空集合ではなく，加法，減法，そして乗法に関して閉じていることを示しさえすればよい．

3.4　次の定理を証明せよ．

定理　体 F の $n+1$ 個の異なる値 $x_0, x_1, \ldots, x_n$ と F の他の $n+1$ 個の値の元 $y_0, y_1, \ldots, y_n$ に対して，$\deg f(x) \leq n$, $f(x_i) = y_i$ を満たすただ 1 つの多項式 $f(x) \in F[x]$ が存在する．

証明は線形代数を用いる．$f(x) = a_0 + a_1x + \cdots + a_nx^n$ とおき，a_i を変数と考える．$f(x_i) = y_i$ を使って次のような $n+1$ 個の連立方程式を考える．

$$\begin{cases} a_0 + a_1x_0 + \cdots + a_nx_0^n = y_0 \\ a_0 + a_1x_1 + \cdots + a_nx_1^n = y_1 \\ \qquad\cdots \\ \qquad\cdots \\ a_0 + a_1x_n + \cdots + a_nx_n^n = y_n \end{cases}$$

この連立方程式（a_i を未知数と考えて）の係数行列はヴァンデルモンドの行列式と呼ばれている．$x_0, \ldots, x_n$ が相異なっていれば，この行列式はゼロではない．したがって，$a_0, \ldots, a_n$ に対するただ 1 組の解が存在する．

(a) $P(0) = 1, P(1) = 1, P(2) = 2, \deg P(x) \leq 2$ を満たすただ 1 つの多項式 $P(x) \in \mathbb{R}[x]$ を求めよ．

(b) $P(0) = 1, P(1) = 2, P(2) = 2, \deg P(x) \leq 2$ を満たすただ 1 つの多項式 $P(x) \in \mathbb{Z}_7[x]$ を求めよ．ここで，$\mathbb{Z}_7$ は 7 を法とする剰余体である．

3.5　(a) 演習問題 3.4 における定理を用いて，次を証明せよ．

F は無限体でかつ，$f(x), g(x) \in F[x]$ とする．任意の $s \in F$ に対して $f(s) = g(s)$ ならば，$f(x)$ と $g(x)$ は同じ多項式である．

(b) このことは，有限体上では必ずしも正しくないことを示せ (ヒント：$\mathbb{Z}_2[x]$ において $f(x) = x + 1, g(x) = x^2 + 1$ を考えよ)．

3.6　除法の定理を用いて，次のそれぞれの多項式環の 2 つの多項式に対する商と剰余を求めよ．

(a) $f(x) = x^3 + 5x^2 + 6x + 1,\ g(x) = x - 1 \in \mathbb{R}[x]$.

(b) $f(x) = x^3 + 5x^2 + 6x + 1,\ g(x) = x - 1 \in \mathbb{Z}_5[x]$.

(c) $f(x) = x^3 + 5x^2 + 6x + 1,\ g(x) = x - 1 \in \mathbb{Z}_{13}[x]$.

3.7　ユークリッドの互除法を用いて，$\mathbb{Q}[x]$ における次のそれぞれの 2 つの多項式の最大公約数を求めよ．

(a) $f(x) = 2x^3 - 4x^2 + x - 2,\ g(x) = x^3 - x^2 - x - 2.$

(b) $f(x) = x^4 + x^3 + x^2 + x + 1,\ g(x) = x^3 - 1.$

3.8　F を K の部分体とする．そのとき，演習問題 3.3 より $F[x]$ は $K[x]$ の部分環である．

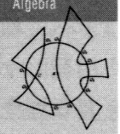
$f(x), g(x), h(x) \in K[x]$ なる多項式に対して，$f(x) = g(x)h(x)$ と仮定する．このとき，これら 3 つの多項式のうちの 2 つが $F[x]$ に属すれば残りの多項式も $F[x]$ に属することを証明せよ．

3.9　$f(x) = x^2 + x + 4$ は $\mathbb{R}[x]$ において既約であり，$\mathbb{C}[x]$ において 1 次因数に分解することを示し，その分解を求めよ．この同じ多項式は $\mathbb{Z}_3[x]$ においても 1 次因数に分解する．その分解を求めよ．

3.10　2 次方程式の根の公式を導き出すことを形式的に実行し，それが標数が 2 と異なる任意の体 F，すなわち，$2 \neq 0$ である体 F 上で成り立つことを示せ（完全平方をつくる操作を使う）．2 についての問題とは何か？

3.11　補題 3.4.2 の (3) を証明せよ．$P(x)$ と $Q(x)$ が複素多項式ならば，$\overline{PQ}(x) = \overline{P}(x)\overline{Q}(x)$ が成り立つことを証明せよ．

3.12　$z \in \mathbb{C}$ ならば，$(x - z)(x - \bar{z}) \in \mathbb{R}[x]$ が成り立つことを証明せよ．



第4章

複素解析学と解析関数

4.1　複素関数と解析性

前節において与えた代数学の基本定理の証明は，2 変数実数値関数の微積分学にのみ基づいていた．しかしながら，その証明はリウヴィルの定理と呼ばれるより一般的な結果を暗示している．この第 6 章で証明される結果より，代数学の基本定理は 1 つの簡単な結論として得られることになる．

これを説明するために，**複素解析学**，あるいは，**複素変数**という基本的な概念を導入しなければならない．それで，微積分学を複素関数に拡張した数学の分野を概観することになる．

複素関数 $w = f(z)$ とは $\mathbb{C} \longrightarrow \mathbb{C}$ なる関数である．ここで，$w, z \in \mathbb{C}$ であり，そのとき，これらを**複素変数**という．幾何学的説明として $\mathbb{C}$ を複素平面とみなせば，複素関数は複素平面から複素平面への**写像**あるいは**変換**である．$z = x + iy = (x, y)$，$w = u + iv$ とおけば $u = u(x, y), v = v(x, y)$ は 2 変数の実数値関数である．したがって，任意の複素関数に付随してこれらの 2 つの変数の実数値関数がある．

$$w = f(z) = u(z) + iv(z). \tag{4.1}$$

関数 $u(z)$ は $f(z)$ の**実部**といい，Re $f(z)$ と表され，また関数 $v(z)$ は $f(z)$ の**虚部**といい，Im $f(z)$ と表される．$f(z)$ についての解析的（微積分学的）な問題は，多くの場合 $u(x, y)$ と $v(x, y)$ についての問題に引き戻されるであろう．

例 4.1.1 複素関数 $f(z) = z^2$ を考える．その実部と虚部を決定せよ．

$z = x + iy$ とおけば $z^2 = (x + iy)^2 = (x^2 - y^2) + i(2xy)$. ゆえに，$\mathrm{Re}\, f(z) = x^2 - y^2$，$\mathrm{Im}\, f(z) = 2xy$. □

微積分学の本質的な概念 —— 連続性，微分可能性，そして積分可能性 —— はすべて極限概念に依存している．したがって，我々の複素解析学もそこから出発しなければならない．しかしながら，複素平面上の位相数学から少し必要な概念を紹介しよう．これは高等微積分学を学んだ読者にとってはなじみがある概念であろう．

$z_0 \in \mathbb{C}$ とするとき，z_0 の **ϵ-開（円）近傍**，は z_0 から距離が ϵ より小さい点の集合であり，これを $N_\epsilon(z_0)$ で表す．すなわち，

$$N_\epsilon(z_0) = \{z \in \mathbb{C}\ ;\ |z - z_0| < \epsilon\}.$$

集合 $U \subset \mathbb{C}$ は，その各点 $z_0 \in U$ について，U に完全に含まれる ϵ-開近傍が存在するとき**開集合**という．集合 $C \subset \mathbb{C}$ は，その補集合 C' が開集合であるとき**閉集合**という．言い換えると，C は $\{z_n\} \subset C$, $z_n \to z$ なる任意の収束点列に対して，$z \in C$ が満たされるとき，閉集合である．集合 $U \subset \mathbb{C}$ は，原点を中心とする半径 r の円板の中に含まれるとき，**有界**であるという．すなわち，ある $r \in \mathbb{R}$ に対して $U \subset \{z\ ;\ |z| \leq r\}$ のとき，U は有界であるという．$\mathbb{C}$ の閉集合かつ有界な部分集合を**コンパクト集合**という．高等微積分学で次のことを学んだ．コンパクト集合 D 上の実数値連続関数は D 上で有界であり，D 上でその最大値，最小値をとる．最後に，開集合 U は，U の任意の 2 つの点が完全に U に含まれている有限個の線分で結ぶことができるとき，**連結**であるという．また，集合 U が連結で，完全に U の中にある単純閉曲線の内部が U の点のみからなるとき，**単連結**という．$\mathbb{C}$ の連結な開集合を**領域**という．図 4.1 と 図 4.2 において，$\mathbb{C}$ の様々な形の部分集合の例を与えた．

次の集合 (図 4.2) は単連結ではない．なぜなら，2 つの穴の 1 つを回る閉曲線はその集合に属していない点を内部に含んでいるからである．

さて，複素関数の極限を，初等微積分学における 1 変数実数値関数に対する方法と本質的にまったく同じやり方で定義しよう．

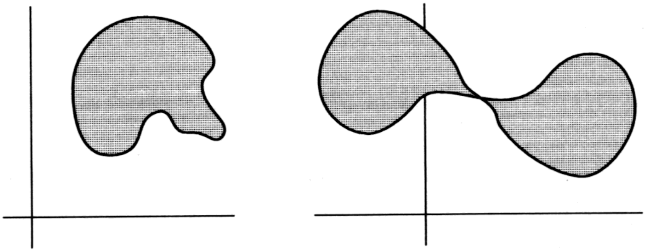


図 4.1 $\mathbb{C}$ のいくつかの部分集合

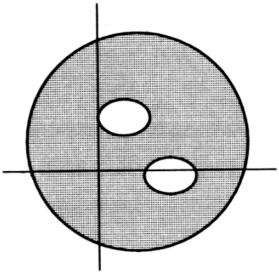


図 4.2 さらなる $\mathbb{C}$ の部分集合

定義 4.1.1 任意の $\epsilon > 0$ に対して，ある正の数 $\delta > 0$ が存在して，$0 < |z - z_0| < \delta$ を満たすすべての複素数 z について $|f(z) - w_0| < \epsilon$ が成り立つときに，$\lim_{z \to z_0} f(z) = w_0$ と表す．

ここでもちろん，距離 $|f(z) - w|$ と $|z - z_0|$ は $\mathbb{C}$ における距離であり，そのとき接近する z は z_0 の ϵ-開近傍の中にある．したがって，無限に多くの接近の仕方がある．

初等微積分学におけるすべての基本的な極限定理 —— 積，和，定数，等 —— がこの状況においても成り立つ．実際に極限を計算するためには実部と虚部に分けて考える．

補題 4.1.1 $f(z) = u(z) + iv(z)$ と表すとき，

$$\lim_{z \to z_0} f(z) = \lim_{z \to z_0} u(z) + i \lim_{z \to z_0} v(z).$$

例 4.1.2　$f(z) = (x^2 + y^2) + i(2xy)$ とする．このとき，$\lim_{z \to 1+i} f(z)$ は次のように計算される．

$$\lim_{z \to 1+i} f(z) = \lim_{(x,y) \to (1,1)} (x^2 + y^2) + i \lim_{(x,y) \to (1,1)} (2xy) = 2 + 2i. \quad \square$$

極限の概念を使うと連続性と微分可能性を定義することができる．

定義 4.1.2　$\lim_{z \to z_0} f(z) = f(z_0)$ が成り立つときに，$w = f(z)$ は z_0 において**連続**であるという．また，複素数の部分集合 U のすべての点において連続であるとき，$f(z)$ は集合 U 上で**連続**であるという．

1 変数の実数値関数の場合における連続性についてのすべての基本的な結果（和と積等）は複素関数においても成り立つ．さらに，極限をとるときに生ずる連続性に関する問題はそれぞれ実部と虚部を調べることによってわかる．

補題 4.1.2　$f(z) = u(z) + iv(z)$ が $z_0 = u(x_0, y_0)$ において連続であるための必要十分条件は $u(x, y)$ と $v(x, y)$ が (x_0, y_0) において連続な 2 変数の実数値関数になることである．

複素多項式は代数的操作によってのみつくられるので，それらは関数 $\mathbb{C} \longrightarrow \mathbb{C}$ とみたとき，$\mathbb{C}$ においていたるところ連続となる．$|z| \to \infty$ のとき $|z^n| \to \infty$ であるから，任意の定数でない複素多項式 $f(z)$ に対して $|z| \to \infty$ のとき $|f(z)| \to \infty$ となる．さらに，$|f(z)|$ はそのとき連続な実数値関数であるから任意のコンパクト集合上で有界である．次にこれらの事実をまとめておく．以下，複素多項式を $\mathbb{C}$ 上の複素関数として考察する．

補題 4.1.3　$f(z) \in \mathbb{C}[z]$ とするとき，次が成り立つ．

(1) $f(z)$ は $\mathbb{C}$ のいたるところで連続である．

(2) $f(z)$ が定数でなければ，$\lim_{z \to \infty} |f(z)| = \infty$.

(3) $|f(z)|$ は $\mathbb{C}$ の任意のコンパクト集合上で有界である．

さて，実数値関数の微分と全く同じ形式的なやり方で複素微分を定義しよう．

定義 4.1.3　$f(z)$ を複素関数とする．$z_0 \in \mathbb{C}$ における**微分係数** $f'(z_0)$ とは次のような極限が存在するときの $f'(z_0)$ のことである．

$$f'(z_0) = \lim_{\Delta z \to 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z}$$

$f'(z_0)$ が存在するとき，$f(z)$ は z_0 で**微分可能**であるという．$f(z)$ が $\mathbb{C}$ の部分集合 U の任意の点において微分可能であるとき，$f(z)$ は U 上で微分可能であるという．

極限と連続性と同様にして，初等的な微積分学におけるすべての基本的な微分の規則 —— 和，積，商，合成関数等 —— は複素関数についても成り立つことが示される．特に，ベキ乗の公式 —— 任意の自然数 n に対して，$f(z) = z^n$ ならば $f'(z) = nz^{n-1}$ が成り立つ —— は定義より純粋に形式的な議論により導かれる．したがって，複素多項式は $\mathbb{C}$ の各点において微分係数をもつ．

補題 4.1.4　$f(z) = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}[z]$ とするとき，各点 z_0 において $f'(z_0)$ が存在し，$f'(z_0) = a_1 + 2a_2 z + \cdots + na_n z^{n-1}$ が成り立つ．$f(z) \in \mathbb{C}[z]$ かつ $\deg f(z) \geq 1$ ならば，$f'(z) \in \mathbb{C}[z]$ かつ $\deg f'(z) = \deg f(z) - 1$ となっている．$f(z) = a_0$ が定数ならば，$f'(z) = 0$ である．

$y = f(x)$ が 1 変数の実数値関数であれば，$f'(x_0)$ は x_0 における接線の勾配を表していた．複素微分係数も幾何学的に説明することが可能である．この説明を 4.3 節で行う．ここでは，さらにいくつかの重要な一般的な概念を導入する．

定義 4.1.4　$w = f(z)$ を複素関数とする．$f(z)$ が z_0 のある ϵ-開近傍において微分可能であるとき，$f(z)$ は z_0 において**解析的**（**正則**）であるという．$f(z)$ が集合 U の任意の点において解析的であるとき，$f(z)$ は U 上で解析的であるという．$f(z)$ が $\mathbb{C}$ 全体で解析的のとき，$f(z)$ は**整関数**という．

補題 4.1.4 より各複素多項式は整関数である．

次の節で，解析性に対する $\mathrm{Re}\, f(z)$ と $\mathrm{Im}\, f(z)$ についての条件を考察する．しかしながら，その前に点 z_0 において複素微分係数は存在するが，z_0 にお

いて解析的ではない関数の例をあげよう．この例を理解するためには次の考えが必要である．

$f(z) = u(z) + iv(z)$ に対して，次のものを定義する．

$$\frac{\partial f}{\partial x} = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x}, \qquad \frac{\partial f}{\partial y} = \frac{\partial u}{\partial y} + i\frac{\partial v}{\partial y}.$$

補題 4.1.5　$w = f(z)$ を実数値をとる複素関数とする．このとき，$f'(z_0)$ が存在すれば，$f'(z_0) = \dfrac{\partial f}{\partial x}(z_0) = \dfrac{\partial f}{\partial y}(z_0)$ が成り立つ．

（証明） 定義より

$$f'(z_0) = \lim_{\Delta z \to 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z}.$$

$f(z)$ は実数値をとるので，$f(z)$ はその実部である $u(z)$ に等しい，つまり，$f(z) = u(z)$. したがって，

$$f'(z_0) = \lim_{(\Delta x, \Delta y) \to (0,0)} \frac{u(x_0 + \Delta x, y_0 + \Delta y) - u(x_0, y_0)}{\Delta z}.$$

$f'(z_0)$ は存在するから，右辺の極限値はその近づき方には無関係である．実軸上に平行な直線に沿って近づけると，$\Delta z = \Delta x, \Delta y = 0$. これらを上の式に代入すると，次を得る．

$$f'(z_0) = \lim_{\Delta x \to 0} \frac{u(x_0 + \Delta x, y_0) - u(x_0, y_0)}{\Delta x} = \frac{\partial u}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial x}(z_0).$$

虚軸上に平行な直線に沿って近づけると，もう 1 つの式の部分を得る．　■

例 4.1.3　$f(z) = |z|^2$ とする．このとき，$f'(0)$ は存在するが，$f(z)$ は $z = 0$ において解析的ではないことを示そう．

$z_0 = 0, f(z) = |z|^2$ と仮定する．このとき，

$$\lim_{\Delta z \to 0} \frac{f(z_0 + \Delta z) - f(z_0)}{\Delta z} = \lim_{\Delta z \to 0} \frac{|\Delta z|^2}{\Delta z} = 0.$$

したがって，$f'(0)$ は存在して $f'(0) = 0$ である．

次に，$f(z)$ は $z=0$ において解析的ではないことを示す．$z=x+iy, |z|^2 = x^2+y^2$ である．$f(z_0)$ が存在すれば，補題 4.1.5 より $f'(z_0) = \dfrac{\partial f}{\partial x}(z_0) = 2x_0 = \dfrac{\partial f}{\partial y}(z_0) = 2y_0$. この式は $x_0 = y_0$ のときだけ成り立つので，その微分係数は z が直線 $y=x$ 上にあるときだけ存在する．ゆえに，その微分係数は 0 の ϵ-開近傍の中では $z=0$ において以外は存在しない．したがって，$f(z)$ は 0 で解析的ではない．次の節で，この関数は 0 においてのみ微分可能であることを証明する． □

4.2 コーシー・リーマンの微分方程式

$f(z) = u(z) + iv(z)$ が z_0 において微分可能であると仮定する．そのとき，

$$f'(z_0) = \lim_{\Delta z \to 0} \frac{u(z_0+\Delta z) + iv(z_0+\Delta z) - (u(z_0)+iv(z_0))}{\Delta z}.$$

この極限は存在するので，この極限は近づき方には無関係に定まる．はじめに，実軸に平行な直線に沿って Δz を 0 に近づける．この場合，$\Delta z = \Delta x, \Delta y = 0$ である．$z_0 = (x_0, y_0)$ とすれば，

$$\begin{aligned}
f'(z_0) &= \lim_{\Delta x \to 0} \frac{u(x_0+\Delta x, y_0) + iv(x_0+\Delta x, y_0) - (u(x_0,y_0)+iv(x_0,y_0))}{\Delta x} \\
&= \lim_{\Delta x \to 0} \frac{u(x_0+\Delta x, y_0) - u(x_0,y_0)}{\Delta x} \\
&\qquad + i \lim_{\Delta x \to 0} \frac{v(x_0+\Delta x, y_0) - u(x_0,y_0))}{\Delta x} \\
&= \frac{\partial u}{\partial x}(z_0) + i\frac{\partial v}{\partial x}(z_0).
\end{aligned}$$

次に，虚軸に平行な直線に沿って Δz を 0 に近づける．この場合，$\Delta z = i\Delta y, \Delta x = 0$ である．そのとき，

$$\begin{aligned}
f'(z_0) &= \lim_{\Delta y \to 0} \frac{u(x_0, y_0+\Delta y) + iv(x_0, y_0+\Delta y) - (u(x_0,y_0)+iv(x_0,y_0))}{i\Delta y} \\
&= \lim_{\Delta y \to 0} \frac{u(x_0, y_0+\Delta y) - u(x_0,y_0)}{i\Delta y} \\
&\qquad + i \lim_{\Delta y \to 0} \frac{v(x_0, y_0+\Delta y) - v(x_0,y_0)}{i\Delta y} \\
&= \frac{\partial v}{\partial y}(z_0) - i\,\frac{\partial u}{\partial y}(z_0).
\end{aligned}$$

微分係数は存在するから，これら 2 つの表現は一致しなければならない．したがって，点 z_0 において次の式が成り立つ．

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

これらの関係式は**コーシー・リーマンの微分方程式**または**コーシー・リーマンの条件**と呼ばれている．この名前は，19 世紀の前半にそれらの関係を発見したコーシーと，同じ 19 世紀の後半にそれらの関係式を複素解析学の理論において基本的なものとしたリーマンに由来している．$u(x,y)$ と $v(x,y)$ が実数値関数のとき，形式的に次のように定義する．

定義 4.2.1　$u(x,y)$ と $v(x,y)$ が次の条件を満たすとき，それらは**コーシー・リーマンの微分方程式**を満たすという．

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

この定義によって次の定理が得られた．

定理 4.2.1　$f(z) = u(z)+iv(z)$ が z_0 において微分可能であれば $\frac{\partial u}{\partial x}, \frac{\partial u}{\partial y}, \frac{\partial v}{\partial x}, \frac{\partial v}{\partial y}$ は z_0 においてすべて存在し，コーシー・リーマンの微分方程式を満たす．さらに，次が成り立つ．

$$f'(z_0) = \frac{\partial u}{\partial x}(z_0) + i\frac{\partial v}{\partial x}(z_0) = \frac{\partial v}{\partial y}(z_0) - i\frac{\partial u}{\partial y}(z_0).$$

一般的に，$f(z)$ がある領域 U において解析的であれば，その実部と虚部は U 全体においてコーシー・リーマンの微分方程式を満たす．さらに，$f(z) = u(z) + iv(z)$ として $u(z), v(z)$ が U において連続な偏導関数をもち，U 全体においてコーシー・リーマンの微分方程式を満たせば，以下に示すように，$f(z)$ は U で解析的である．

$z_0 \in U$ とする．$f'(z_0)$ が存在することを示さなければならない．次の極限を考える．

$$\begin{aligned}
&\lim_{\Delta z \to 0} \frac{u(z_0 + \Delta z) + iv(z_0 + \Delta z) - (u(z_0) + iv(z_0))}{\Delta z} \\
&\quad = \lim_{\Delta z \to 0} \frac{\Delta u + i\Delta v}{\Delta z} = \lim_{\Delta z \to 0} \frac{\Delta u}{\Delta z} + i \lim_{\Delta z \to 0} \frac{\Delta v}{\Delta z}.
\end{aligned}$$

$u(x,y), v(x,y)$ は (x_0, y_0) において連続な偏導関数をもつので，次のように表せる．

$$\Delta u = \frac{\partial u}{\partial x}\Delta x + \frac{\partial u}{\partial y}\Delta y + \epsilon_1 \Delta x + \epsilon_2 \Delta y$$
$$\Delta v = \frac{\partial v}{\partial x}\Delta x + \frac{\partial v}{\partial y}\Delta y + \epsilon_3 \Delta x + \epsilon_4 \Delta y$$

ここで，$(\Delta x, \Delta y) \to (0,0)$ のとき $\epsilon_i \to 0 (i = 1,2,3,4)$ である．

したがって，コーシー・リーマンの微分方程式より

$$\lim_{\Delta z \to 0} \frac{\Delta u + i\Delta v}{\Delta z}$$
$$= \lim_{\Delta z \to 0} \frac{1}{\Delta z}\left(\frac{\partial u}{\partial x}(\Delta x + i\Delta y) + i\frac{\partial v}{\partial x}(\Delta x + i\Delta y) + \delta_1 \Delta x + \delta_2 \Delta y\right).$$

$\Delta z = \Delta x + i\Delta y$ であるから，上の式は次のようになる．

$$\lim_{\Delta z \to 0}\left(\frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x} + \delta_1 \frac{\Delta x}{\Delta z} + \delta_2 \frac{\Delta y}{\Delta z}\right).$$

ここで，$\Delta z \to 0$ のとき $\delta_1, \delta_2 \to 0$ である．

$|\Delta x| \leq |\Delta z|$ かつ $|\Delta y| \leq |\Delta z|$ であるから，$|\frac{\Delta x}{\Delta z}| \leq 1, |\frac{\Delta y}{\Delta z}| \leq 1$. ゆえに，上の極限の式において後の 2 つの項は Δz とともに 0 に近づく．したがって，z_0 において次の式が成り立つ．

$$f'(z_0) = \frac{\partial u}{\partial x}(z_0) + i\frac{\partial v}{\partial x}(z_0).$$

ゆえに，$f'(z)$ は z_0 において微分可能である．

上で調べたことをまとめて，次の定理とその系を得る．

定理 4.2.2

(1) $f(z) = u(z) + iv(z)$ とする．$z_0 = (x_0, y_0)$ において $f'(z_0)$ が存在すれば，$u(x,y), v(x,y)$ の (x_0, y_0) における偏微分係数は存在してコーシー・リーマンの微分方程式を満足する．

(2) $f(z) = u(z) + iv(z)$ とする．$u(x,y), v(x,y)$ とそれらの偏導関数が $z_0 = (x_0, y_0)$ において連続でかつ (x_0, y_0) においてコーシー・リーマンの微分方程式を満足すれば，$f'(z_0)$ が存在する．すなわち，$f'(z)$ は z_0 において微分可能である．

系 4.2.1 $f(z) = u(z) + iv(z)$ として，$u(x, y), v(x, y)$ とそれらの偏導関数が $\mathbb{C}$ のある領域において連続であると仮定する．このとき，$f(z)$ が U 上で解析的であるための必要十分条件は u, v がコーシー・リーマンの微分方程式を満足することである．

例 4.2.1 $f(z) = e^x \cos y + ie^x \sin y$ とする．このとき，$f(z)$ はいたるところで解析的であり，$f'(z) = f(z)$ であることを示せ．

ここで，$u(x, y) = e^x \cos y, v(x, y) = e^x \sin y$ である．これらの関数はいたるところで連続で微分可能な 2 変数の実数値関数である．それゆえ，$f(z)$ が解析的であることを示すには，それらがコーシー・リーマンの微分方程式を満足することを示せば十分である．さて，

$$\frac{\partial u}{\partial x} = e^x \cos y,\ \frac{\partial u}{\partial y} = -e^x \sin y,\ \frac{\partial v}{\partial x} = e^x \sin y,\ \frac{\partial v}{\partial y} = e^x \cos y.$$

したがって，$\mathbb{C}$ のすべての点で $\dfrac{\partial u}{\partial x} = \dfrac{\partial v}{\partial y}, \dfrac{\partial v}{\partial x} = -\dfrac{\partial u}{\partial y}$ が成り立つ．ゆえに，$f(z)$ は $\mathbb{C}$ においていたるところ解析的である．

さらに，$f'(z) = \dfrac{\partial u}{\partial x} + i\dfrac{\partial v}{\partial x} = e^x \cos y + ie^x \sin y = f(z)$. □

この例で考えている関数は実際**複素指数関数** $f(z) = e^z$ である．このことを見るために，$z = x + iy,\ x, y \in \mathbb{R}$ とおく．このとき，$e^z = e^{x+iy}$. すると，オイラーの等式により $e^z = e^x e^{iy} = e^x(\cos y + i \sin y) = e^x \cos y + ie^x \sin y$. この例によって，指数関数に対して我々が期待しているように，$f(z) = e^z$ ならば $f'(z) = e^z$ となるのである．

例 4.2.2 コーシー・リーマンの微分方程式を用いて，$f(z) = z^2$ はいたるところ正則であって，$f'(z) = 2z$ となることを示せ．

$z = x + iy$ とおけば，$f(z) = z^2 = (x + iy)^2 = x^2 - y^2 + i(2xy)$. このとき，$u(x, y) = x^2 - y^2, v(x, y) = 2xy$ である．偏導関数を計算すると，

$$\frac{\partial u}{\partial x} = 2x,\ \frac{\partial u}{\partial y} = -2y,\ \frac{\partial v}{\partial x} = 2y,\ \frac{\partial v}{\partial y} = 2x.$$

明らかに，これらの関数は連続であり，$\mathbb{C}$ 全体でコーシー・リーマンの微分方程式を満足する．ゆえに，$f(z)$ はいたるところ解析的である．さらに，

$$f'(z) = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x} = 2x + i(2y) = 2(x+iy) = 2z. \qquad \square$$

系 4.2.2

(1) 実数値のみをとる解析関数は定数となる．

(2) ある領域 U 上で $f'(z) = 0$ であれば，$f(z)$ は定数である．

（証明）

(1) $f(z)$ が実数値関数とする．そのとき，$f(z) = u(z)$ であり，$v(z) = 0$ となる．$f(z)$ は解析的であるから，コーシー・リーマンの微分方程式を満足するので $\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} = 0, \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x} = 0$. ゆえに，$\frac{\partial u}{\partial x} = \frac{\partial u}{\partial y} = 0$. したがって，$u(x,y)$ は定数となるから $f(z)$ も定数である．

(2) $f' = 0$ とすると，$f' = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x} = \frac{\partial v}{\partial y} - i\frac{\partial u}{\partial y} = 0$. この式は $\frac{\partial u}{\partial x} = \frac{\partial u}{\partial y} = \frac{\partial v}{\partial x} = \frac{\partial v}{\partial y} = 0$ を意味している．ゆえに，$u(x,y)$ と $v(x,y)$ は 2 つとも定数となるから，$f(z)$ も定数である． ■

例 4.1.3 において，関数 $f(z) = |z|^2$ は 0 において微分可能ではあるが，0 において解析的ではないことを示した．この関数は実数値関数で，しかも定数ではない．ゆえに上の結果より，どの点においても解析的でないことがわかる．

定義 4.2.2 実数値関数 $u(x,y)$ は，連続な第 2 次偏導関数をもち，次の**ラプラスの方程式**を満たすとき，**調和関数**であるという．

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0.$$

この定義によって，解析関数の 1 つの性質は次のように表現される．

補題 4.2.1 $f(z) = u(x,y) + iv(x,y)$ が解析関数であれば，$u(x,y)$ と $v(x,y)$ は調和関数である．

（証明）第 2 次偏導関数の連続性については後に残しておく．$f(z)$ が解析的であると仮定する．そのとき，$f(z)$ はコーシー・リーマンの微分方程式

$\dfrac{\partial u}{\partial x}=\dfrac{\partial v}{\partial y}$ と $\dfrac{\partial u}{\partial y}=-\dfrac{\partial v}{\partial x}$ を満たしている．また連続な第 2 次偏導関数が存在するので，偏微分の順序を交換することができる．このことより，

$$\frac{\partial^2 u}{\partial x^2}=\frac{\partial^2 v}{\partial y\partial x}=\frac{\partial^2 v}{\partial x\partial y}=-\frac{\partial^2 u}{\partial y^2}.$$

したがって，$\dfrac{\partial^2 u}{\partial x^2}=-\dfrac{\partial^2 u}{\partial y^2}$ となる．すなわち，$\dfrac{\partial^2 u}{\partial x^2}+\dfrac{\partial^2 u}{\partial y^2}=0$ である．ゆえに，$u(x,y)$ は調和関数となる．同様の議論によって，$v(x,y)$ も調和関数であることがわかる． ■

この補題における u と v を**共役調和関数**という．

例 4.2.3 $u(x,y)=y^3-3x^2y$ は調和関数であることを示し，$f(z)=u+iv$ が正則関数となるように共役調和関数 $v(x,y)$ を求めよ．

$\dfrac{\partial u}{\partial x}=-6xy, \dfrac{\partial u}{\partial y}=3y^2-3x^2$ であるから，$\dfrac{\partial^2 u}{\partial x^2}=-6y, \dfrac{\partial^2 u}{\partial y^2}=6y$. ゆえに，$\dfrac{\partial^2 u}{\partial x^2}+\dfrac{\partial^2 u}{\partial y^2}=0$. したがって，$u(x,y)$ は調和関数である．

$v(x,y)$ を $u(x,y)$ の共役調和関数とする．コーシー・リーマンの微分方程式より，

$$\frac{\partial u}{\partial x}=\frac{\partial v}{\partial y},\ \frac{\partial u}{\partial y}=-\frac{\partial v}{\partial x}.$$

はじめに，$\dfrac{\partial v}{\partial y}=\dfrac{\partial u}{\partial x}=-6xy$ を考えて，y について積分すると

$$v(x,y)=-3xy^2+g(x)$$

を得る．ここで，$g(x)$（積分定数）は x のみの関数である．すると，

$$\frac{\partial v}{\partial x}=-3y^2+g'(x)=-\frac{\partial u}{\partial y}=-3y^2+3x^2.$$

この式より，$g'(x)=3x^2$ が得られるので，これを x について積分すると $g(x)=x^3+c$ を得る．c は任意の定数であるから，$c=0$ とすれば，$v(x,y)=x^3-3xy^2$ が $u(x,y)$ の共役調和関数である．そして，

$$f(z)=(y^3-3x^2y)+i(x^3-3xy^2)$$

は解析関数である． □

4.3　等角写像と解析性

初等微積分学において次のことを学んだことを思い起こそう．1変数の微分可能な実数値関数 $y = g(x)$ の微分係数 $g'(x_0)$ は曲線 $y = g(x)$ の点 $(x_0, g(x_0))$ における接線の勾配を表している．したがって， $g'(x_0)$ は次のような幾何学的情報を与えてくれる．それは第一に，その曲線がその点において動いていく方向，すなわち，角度であり，第二に，その大きさはその曲線の瞬間的な変化率である．複素偏微分係数，したがって解析性もまた，以下において考察するように幾何学的に解釈される．

定義 4.3.1　$\mathbb{C}$ における**曲線**とは

$$\gamma(t) = x(t) + iy(t) \tag{4.3.1}$$

によって与えられる連続関数 $\gamma : [a, b] \longrightarrow \mathbb{C}$ のことである．ここで，$x(t), y(t)$ は実数の区間 $[a, b]$ 上の実数値関数である．$x(t), y(t)$ が t_0 で微分可能であるとき，γ は t_0 で**微分可能な曲線**といい，そのとき $\gamma'(t_0) = x'(t_0) + iy'(t_0)$ である．すべての点に対して微分可能であるとき，曲線は**微分可能**であるという．曲線は，微分可能であって，かつその導関数もまた $[a, b]$ 上で連続であるとき，**連続的微分可能**であるという．曲線 $\gamma(t)$ は，$\gamma'(t_0) \neq 0$ であるとき，t_0 で**正則**であるという．正則点 t_0 における $\gamma(t)$ の**方向**とは $\mathrm{Arg}\,\gamma'(t_0)$ のことである．一般に，すべての点で正則な曲線を**正則曲線**という．

例 4.3.1　曲線　$\gamma(t) = r\cos t + ir\sin t,\ 0 \leq t \leq 2\pi$ は原点を中心として，半径 r の円を表す．

導関数は　$\gamma'(t) = -r\sin t + ir\cos t$, これが決して 0 にならないので，$\gamma(t)$ はすべての t について正則である．

$t = 0$ で $\gamma'(0) = ir$. これは純虚数であるから，図 4.3 における図を見てわかるように，その偏角は $\pi/2$ である．

さらに一般的に，z_0 を中心とする半径 r の円は

$$\gamma(t) = z_0 + re^{it},\ 0 \leq t \leq 2\pi \tag{4.3.2}$$

によって表される．この表現は後で必要となる．

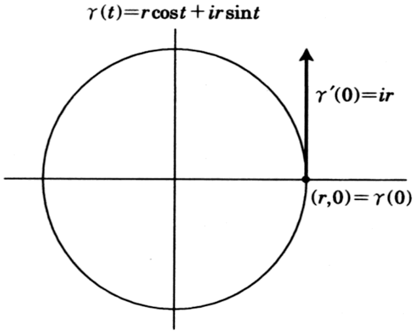


図 4.3　$\mathbb{C}$ における円

γ_1, γ_2 を $\gamma_1(t_1) = \gamma_2(t_2)$ を満たす $\mathbb{C}$ の 2 つの曲線で，γ_1 と γ_2 はそれぞれ t_1, t_2 で正則であると仮定する．そのとき，この共通点における γ_1 から γ_2 への**角**は $\mathrm{Arg}\,\gamma_2'(t_2) - \mathrm{Arg}\,\gamma_1'(t_1)$ である．

さらに，$\gamma(t)$ が領域 $U \subset \mathbb{C}$ に値をとる曲線とし，$F : U \to \mathbb{C}$ とする．このとき，$F \circ \gamma$ もまた 1 つの曲線である．F が複素導関数をもち，γ が t_0 で微分可能であれば，$(F \circ \gamma)'(t_0) = F'(\gamma(t_0))\gamma'(t_0)$. γ が t_0 で正則で $F'(\gamma(t_0)) \neq 0$ ならば，$F \circ \gamma$ は t_0 で正則である．□

定義 4.3.2　$U \subset \mathbb{C}$ で $F : U \to \mathbb{C}$ とする．$t_0 \in U$ で正則である任意の曲線 γ に対して，$\gamma(t_0) = z_0$ とし，$F \circ \gamma$ がまた t_0 で正則であり，かつ F が z_0 において**角を保存**するとき，F は z_0 で**等角**であるという．角を保存するということは，$\gamma_1(t), \gamma_2(t)$ を U に値をとる 2 つの曲線で，$\gamma_1(t) = \gamma_2(t) = z_0$ であるとき，z_0 における γ_1 から γ_2 への角度が $F(z_0)$ における $F \circ \gamma_1$ から $F \circ \gamma_2$ への角度と等しいということを意味している．F が U 上いたるところで等角であるとき，F を**等角写像**という．

等角性と解析性との間の関係は次の定理と系によって具体化される．

定理 4.3.1

(1) 領域 $U \subset \mathbb{C}$ 上の連続な複素関数 $f(z)$ が z_0 において 0 でない複素微分係数をもてば，$f(z)$ は z_0 において等角である．

(2) $f(z)$ が領域 $U \subset \mathbb{C}$ 上で連続でありかつ $z_0 \in U$ で等角であるとする．

さらに，z_0 でその 2 つの偏導関数が存在して連続であると仮定する．そのとき，$f'(z_0)$ が存在して，それは 0 ではない．

（**証明**）(1) を証明し，(2) の証明の概要は演習問題に残しておく．

$f(z)$ を z_0 において 0 でない微分係数をもつ連続な複素関数とする．f が z_0 で等角であることを示そう．

γ_1, γ_2 を U に値をとる 2 つの正則な曲線で，$\gamma_1(t_1) = \gamma_2(t_2) = z_0$ であるとする．$f'(z_0) \neq 0$ であるから，$f \circ \gamma_1$ と $f \circ \gamma_2$ は t_1, t_2 において正則である．そのとき，$f(z_0)$ における $f \circ \gamma_1$ から $f \circ \gamma_2$ への角度は

$$\begin{aligned}&\mathrm{Arg}((f \circ \gamma_2)'(t_2)) - \mathrm{Arg}((f \circ \gamma_1)'(t_1))\\&\quad = \mathrm{Arg}(f'(\gamma_2(t_2))\gamma_2'(t_2)) - \mathrm{Arg}(f'(\gamma_1(t_1))\gamma_1'(t_1)).\end{aligned}$$

任意の $z, w \in \mathbb{C}$ に対して，$\mathrm{Arg}(zw) = \mathrm{Arg}(z) + \mathrm{Arg}(w)$ が成り立つことを思い出そう．それゆえ，上の式は次のようになる．

$$\mathrm{Arg}(f'(\gamma_2(t_2))) + \mathrm{Arg}(\gamma_2'(t_2)) - \mathrm{Arg}(f'(\gamma_1(t_1))) - \mathrm{Arg}(\gamma_1'(t_1)).$$

ここで，$\gamma_2(t_2) = \gamma_1(t_1)$ であるから上の式は次式に等しくなる．

$$\mathrm{Arg}(\gamma_2'(t_2)) - \mathrm{Arg}(\gamma_1'(t_1)).$$

これは，z_0 における γ_1 から γ_2 への角度である．ゆえに，$f(z)$ は z_0 における角度を保存し，したがって z_0 で等角である．■

系 4.3.1　すべての偏導関数が存在してそれらが連続である，連続な複素関数 $f(z)$ がある領域 $U \subset \mathbb{C}$ 上で等角写像であるための必要十分条件は，$f(z)$ が U 上で解析的でかつ U 上で $f'(z) \neq 0$ なることである．

（**証明**）$f(z)$ が解析的でかつ $f(z) \neq 0$ とすれば，各点 $z_0 \in U$ において $f'(z_0) \neq 0$ である．そのとき，定理 4.3.1 の (1) より $f(z)$ は z_0 で等角であり，ゆえに U 上で等角写像である．

逆に，$f(z)$ が U の各点で連続でかつ等角であると仮定する．そのとき同じ定理の (2) より $f'(z_0)$ は存在し，各 $z_0 \in U$ において 0 ではない．したがって，$f(z)$ は U 上で解析的でかつ $f'(z) \neq 0$ である．■

等角性は実関数の導関数を方向の測度として考える使い方に類似している．複素関数においてもこの瞬間変化率に対応する概念がある．

定義 4.3.3 $f : U \to \mathbb{C}, U \subset \mathbb{C}, z_0 \in U$ でまた，$M \geq 0$ と仮定する．$f(z)$ は次の極限が存在するとき，z_0 において M 倍の**拡大**であるという．

$$\lim_{\Delta z \to 0} \frac{|f(z_0 + \Delta z) - f(z_0)|}{|\Delta z|} = M.$$

明らかに，$f'(z_0)$ が存在すれば，$f(z)$ は z_0 において $|f'(z_0)|$ 倍の拡大である．しかしその逆については，次の定理の (2) として述べるように，これに対する部分的な逆が成り立つ．

定理 4.3.2

(1) $f(z)$ が z_0 で微分可能ならば，$f(z)$ は z_0 で $|f'(z_0)|$ 倍の拡大である．

(2) U を $\mathbb{C}$ における領域とし，$f(z)$ を U 上の連続な複素関数とする．$z_0 \in U, M \geq 0$ として $f(z)$ を z_0 において M 倍の拡大とし，さらに，z_0 ですべての偏導関数が存在して連続であり，$z_0 = \gamma(t_0)$ を満たすとき，t_0 で微分可能な任意の曲線 γ に対して，$f \circ \gamma$ は t_0 で微分可能であると仮定する．そのとき，$f(z)$ が z_0 で微分可能であるか，または $\bar{f}(z)$ が z_0 で微分可能である．

例 4.3.2 $f(z) = e^z$ とする．このとき，$f(z)$ は $\mathbb{C}$ 全体で等角写像であることを示せ．

$f(z) = e^z = e^x \cos y + ie^x \sin y$ とする．$f(z)$ は $\mathbb{C}$ において決して 0 にならない．例 4.2.1 において $f'(z) = e^z$ であることを示した．したがって，$\mathbb{C}$ において $f'(z) \neq 0$. ゆえに，$f(z)$ は等角写像である．

さらに，$f(z) = e^z$ は帯 $-\pi < y < \pi$ を 1 対 1 かつ等角に原点と負の実軸を除いた裂け目のある平面に移す．これを図 4.4 に示してある．□

演習問題

4.1　$f(z) = z^3$ とするとき，次の問に答えよ．

(a) $f(z)$ の実部と虚部を求めよ．

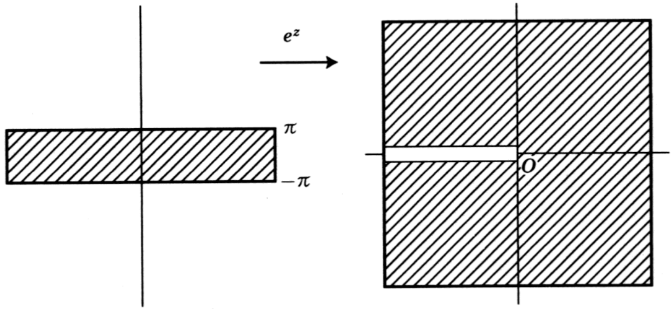


図 4.4　等角写像としての e^z

(b) コーシー・リーマンの微分方程式を用いて，$f(z)$ がいたるところ解析的であり $f'(z) = 3z^2$ であることを示せ．

(c) z^3 について，定義より直接に（初等解析学におけるように）$f'(z) = 3z^2$ であることを示せ．

4.2　帰納法と積の公式を用いて，$f(z) = z^n$ $(n \in \mathbb{N})$ ならば $f'(z) = nz^{n-1}$ であることを示せ．

4.3　関数 $f(z) = \bar{z}$ は $\mathbb{C}$ 上どの点においても微分可能ではないことを示せ．

4.4　$f(z)$ を解析関数とする．このとき，$f(z)$ が定数でなければ，$g(z) = \overline{f(z)}$ は解析関数ではないことを示せ．

4.5　$f(z) = (2x^2 + y) + i(x^3 - y^3)$ とするとき，次の問に答えよ．

(a) $f(i + 2i)$ を求めよ．

(b) $\lim_{z \to 3-i} f(z)$ を求めよ．

(c) $f(z)$ は（もしあるとすれば）どの点で微分可能か．

(d) $f(z)$ は $\mathbb{C}$ 上いたるところで解析的か．またそれはなぜか．

4.6　次の関数は整関数であることを示せ．

(a) $f(z) = (3x + y) + i(3y - x)$.

(b) $f(z) = e^{-y} \cos x + ie^{-y} \sin x$.

4.7　次の関数はどの点においても解析的でないことを示せ．

(a) $f(z) = xy + iy$.

(b) $f(z) = e^{y} \cos x + ie^{y} \sin x$. ここで，複素指数関数について演習問題 4.6 との違いに注意せよ．

4.8　次のそれぞれの関数が調和関数になることを示し，それぞれの共役調和

関数を求めよ.

(a) $u(x,y) = 2x - 2xy$.

(b) $u(x,y) = 2x - x^3 + 3xy^2$.

4.9　次の曲線はどのような形になるか，概形を描け.

(a) $\gamma(t) = (3+i) + 4e^{it},\ 0 \le t \le 2\pi$.

(b) $\gamma(t) = t + it^2,\ 0 \le t \le 1$.

(c) $\gamma(t) = t^2 + i\log t,\ 1 \le t \le 2$.

4.10　$\gamma_1(t) = t + it^2\ (0 \le t \le 1)$, $\gamma_2(t) = \dfrac{1}{2} + \dfrac{1}{4}e^{it}\ (0 \le t \le 2\pi)$ とする．そのとき，$\gamma_1(1/2) = \gamma_2(\pi/2) = z_0$ である．この共通点における 2 つの曲線のなす角を求めよ.

4.11 (a) $\lim_{z\to z_0} f(z) = w_1$, $\lim_{z\to z_0} g(z) = w_2$ ならば，$\lim_{z\to z_0}(f(z)+g(z)) = w_1 + w_2$ が成り立つことをきちんと証明せよ.

(b) $f(z)$ と $g(z)$ が z_0 で連続であれば，$f(z)+g(z)$ も z_0 で連続であることを (a) を用いて示せ.

4.12　複素三角関数は次のように定義される.

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}, \quad \cos z = \frac{e^{iz} + e^{-iz}}{2}.$$

(a) オイラーの等式 $e^{it} = \cos t + i\sin t$ を複素数に適用して，上の定義は期待するような事柄を満たすことを示せ.

(b) 複素指数関数の導関数を用いて，三角関数の導関数を求めよ．すなわち，$f(z) = \sin z$ とすれば $f'(z) = \cos z$ であり，$f(z) = \cos z$ とすれば $f'(z) = -\sin z$ であることを示せ.

この後の 2 つの問題は定理 4.3.1 の (2) の証明の概略を示している．すなわち，$f(z)$ が z_0 で等角であれば，$f(z)$ は z_0 で微分可能であり，$f'(z_0) \ne 0$ であることの証明の概略である.

4.13　作用素 $\dfrac{\partial}{\partial \bar{z}}$ を次のように定義する.

$$\frac{\partial}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right).$$

$f(z) = u(z) + iv(z)$ を z_0 を含んでいる領域で連続であるとする．z_0 で偏導関数が存在し連続であると仮定する．このとき，$f(z)$ が z_0 で微分可能であることは z_0 で $\dfrac{\partial f}{\partial \bar{z}} = 0$ なることと同値であることを証明せよ

(ヒント：$\dfrac{\partial f}{\partial \bar{z}}$ を展開して，コーシー・リーマンの微分方程式と比較せよ).

4.14 γ は t_0 で正則な曲線とし, $z_0 = \gamma(t_0)$ とおく．また，連続関数 $f(z)$ は z_0 で偏導関数が存在し連続であると仮定する．さらに，$f \circ \gamma$ もまた t_0 で解析的であるとする．このとき，次の式が成り立つことを示せ．

$$(f \circ \gamma)'(t_0) = \frac{\partial f}{\partial z}(z_0)\gamma'(t_0) + \frac{\partial f}{\partial \bar{z}}(z_0)\overline{\gamma'(t_0)}.$$

ここで，作用素は　$\dfrac{\partial}{\partial z} = \dfrac{1}{2}(\dfrac{\partial}{\partial x} - i\dfrac{\partial}{\partial y})$.

さて，ここで定理 4.3.1 (2) の証明を与えよう．任意の実数 θ に対して，曲線 $\gamma_\theta(t) = z_0 + te^{i\theta}$ を定義する．そのとき，任意の θ に対して $z_0 = \gamma_\theta(0)$ でかつ　$\gamma_\theta'(t) = e^{i\theta}$. さらに，すべての実数 θ, ϕ に対して z_0 における γ_θ から γ_ϕ への角度は　$\phi - \theta$ である．

$f(z)$ は z_0 で等角であるから，次が成り立つ．

$$\phi - \theta = \mathrm{Arg}(f \circ \gamma_\phi)'(t_0) - \mathrm{Arg}(f \circ \gamma_\theta)'(t_0).$$

演習問題 4.14 を用いて，展開し整理すると次を得る．

$$\phi - \theta = \phi - \theta + \mathrm{Arg}\left(\frac{\partial f}{\partial z} + e^{-2i\phi}\frac{\partial f}{\partial \bar{z}}\right) - \mathrm{Arg}\left(\frac{\partial f}{\partial z} + e^{-2i\theta}\frac{\partial f}{\partial \bar{z}}\right).$$

したがって，

$$\mathrm{Arg}\left(\frac{\partial f}{\partial z} + e^{-2i\phi}\frac{\partial f}{\partial \bar{z}}\right) = \mathrm{Arg}\left(\frac{\partial f}{\partial z} + e^{-2i\theta}\frac{\partial f}{\partial \bar{z}}\right).$$

$\theta = 0$ とおけば，中心が $\dfrac{\partial f}{\partial z}$ で半径 $|\dfrac{\partial f}{\partial \bar{z}}|$ であるすべての円は $\mathrm{Arg}(z) = \mathrm{Arg}\left(\dfrac{\partial f}{\partial z} + \dfrac{\partial f}{\partial \bar{z}}\right)$ なる角度の放射線の中に含まれる．これが可能なのは半径が 0 である場合だけである．ゆえに，$|\dfrac{\partial f}{\partial \bar{z}}| = 0$. したがって，演習問題 4.13 より，$f(z)$ は微分可能である．

第5章

複素積分とコーシーの定理

5.1 線積分とグリーンの定理

前の章において，微分という概念を複素関数にまで拡張した．同様に，積分の概念を適切な複素積分の理論に拡張しよう．この拡張された理論により，代数学の基本定理の第 2 の証明を与えることができる．

$z = f(x, y)$ を 2 変数の実数値関数とすれば，積分についての 2 つの適切な概念があることを思い起こそう．第 1 は集合 R 上の **2 重積分** $\iint_R f(x, y)dA$ である．この積分は面積に関係しており，2 次元の集合上の 2 変数関数の積分である．第 2 は 2 重積分にかえて，1 次元の集合 —— 曲線 —— 上の 2 変数関数の積分である**線積分**を用いる．複素積分にとって最も適切なものはこの第 2 の積分である線積分である．以下，この節において実線積分の基本的な考えを見ていこう．

定義 5.1.1 U を xy-平面上の領域，γ を U に含まれる曲線，そして $f(x, y)$ を U 上で定義された実数値関数とする．図 5.1 におけるように γ を分割した γ 上のひとつながりの点 $P_0 = (x_0, y_0), P_1 = (x_1, y_1), \ldots, P_n = (x_n, y_n)$ を選ぶ．

そのとき，$f(P_i) = f(x_i, y_i)$ が定義される．$\Delta x_i = x_i - x_{i-1}$ とおき，リーマン和 $\sum_{i=1}^{n} f(x_i, y_i)\Delta x_i$ をつくる．このとき，分割した点の選び方に無関係に次の式で表される極限が存在するとき，この極限を x に関する γ 上の

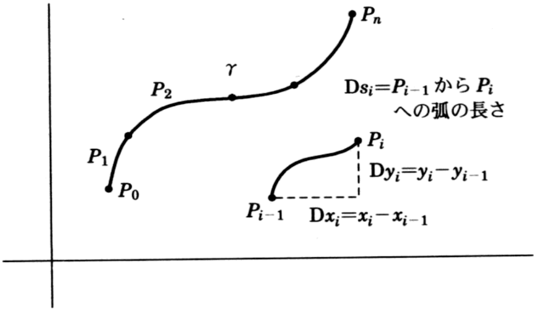


図 **5.1** 線積分

$f(x,y)$ の**線積分**といい，$\int_\gamma f(x,y)dx$ と表す．

$$\int_\gamma f(x,y)dx = \lim_{\Delta x_i \to 0} \sum_{i=1}^{n} f(x_i, y_i)\Delta x_i. \tag{5.1.1}$$

同様にして，$\Delta y_i = y_i - y_{i-1}$ とおけば，y に関する γ 上の $f(x,y)$ の**線積分**は次のように定義される．

$$\int_\gamma f(x,y)dy = \lim_{\Delta y_i \to 0} \sum_{i=1}^{n} f(x_i, y_i)\Delta y_i. \tag{5.1.2}$$

最後に，Δs_i を γ に沿って P_{i-1} から P_i への弧の長さとすれば**弧長に関する** γ 上の $f(x,y)$ の**線積分**は次のように定義される．

$$\int_\gamma f(x,y)ds = \lim_{\Delta s_i \to 0} \sum_{i=1}^{n} f(x_i, y_i)\Delta s_i. \tag{5.1.3}$$

領域 U 上における $f(x,y)$ の連続性と曲線の連続的微分可能性という条件は線積分の存在にとって十分である．

補題 5.1.1 $f(x,y)$ が U 上連続であり $\gamma \subset U$ が連続的微分可能であれば，上で述べた線積分は存在する．

上で述べた種々の線積分は普通の積分にもどって計算することができる．$\gamma(t) = x(t) + iy(t) = (x(t), y(t)), t_0 \le t \le t_1$ と仮定する．そのとき，$dx =$

$x'(t)dt, dy = y'(t)dt, ds = \sqrt{x'(t)^2 + y'(t)^2}dt$. これらを代入して，次を得る．

$$\int_\gamma f(x,y)dx = \int_{t_0}^{t_1} f(x(t),y(t))x'(t)dt. \tag{5.1.1'}$$

$$\int_\gamma f(x,y)dy = \int_{t_0}^{t_1} f(x(t),y(t))y'(t)dt. \tag{5.1.2'}$$

$$\int_\gamma f(x,y)ds = \int_{t_0}^{t_1} f(x(t),y(t))\sqrt{x'(t)^2 + y'(t)^2}dt. \tag{5.1.3'}$$

さらに，曲線 γ が具体的に $y = g(x)$ で $x = a$ から $x = b$ として与えられれば，$dx = dx, dy = g'(x)dx, ds = \sqrt{1 + g'(x)^2}dx$. したがって，上の式は次のようになる．

$$\int_\gamma f(x,y)dx = \int_a^b f(x,g(x))dx. \tag{5.1.1''}$$

$$\int_\gamma f(x,y)dy = \int_a^b f(x,g(x))g'(x)dx. \tag{5.1.2''}$$

$$\int_\gamma f(x,y)ds = \int_a^b f(x,g(x))\sqrt{1 + g'(x)^2}dx. \tag{5.1.3''}$$

以下，この章においては連続的に微分可能な曲線のみを考える．ゆえに，曲線という言葉は連続的微分可能曲線を意味するものとする．

次のいくつかの例の中で，以上の計算について説明しよう．

例 5.1.1　線積分 $\int_\gamma 2xydx + (x^2 - y^2)dy$ を計算せよ．ただし，γ は $x(t) = t^2 - 1, y(t) = t^2 + 1, 0 \leq t \leq 1$ によって与えられる曲線とする．

$dx = 2tdt, dy = 2tdt$ であるから，

$$\int_\gamma 2xydx + (x^2 - y^2)dy$$
$$= \int_0^1 2(t^2 - 1)(t^2 + 1)2tdt + \int_0^1 ((t^2 - 1)^2 - (t^2 + 1)^2)2tdt = -\frac{10}{3}. \quad \square$$

例 5.1.2 線積分 $\int_\gamma (y^3 - 3xy^2)dy$ を計算せよ．ただし，γ は $y = 2x^2, 0 \leq x \leq 1$ によって与えられる曲線とする．

$dy = 4xdx$ であるから,

$$\int_\gamma (y^3 - 3xy^2)dy = \int_0^1 ((2x^2)^3 - 3x(2x^2)^2)4xdx$$
$$= \int_0^1 (32x^7 - 48x^6)dx = -\frac{20}{7}. \qquad \square$$

例 5.1.3 線積分 $\int_\gamma yds$ を計算せよ．ただし，γ は $y = g(x) = \sqrt{x}, 0 \leq x \leq 6$ によって与えられる曲線とする．

$ds = \sqrt{1 + g'(x)^2}dx = \frac{1}{2}\sqrt{\frac{1+4x}{x}}dx$ であるから,

$$\int_\gamma yds = \frac{1}{2}\int_0^6 \sqrt{x}\sqrt{\frac{1+4x}{x}}dx$$
$$= \frac{1}{2}\int_0^6 (1+4x)^{\frac{1}{2}}dx = \frac{31}{3}. \qquad \square$$

線積分は物理学において次のような文脈の中でしばしば現れる．$\overrightarrow{F(x,y)} = P(x,y)\boldsymbol{i} + Q(x,y)\boldsymbol{j}$ を平面上を動く連続的なベクトル関数とする (ここで，$\boldsymbol{i}$ と $\boldsymbol{j}$ は標準的な単位ベクトルである)．そのとき，ある粒子をこの力に従って曲線上に沿って押したときになされる仕事は次のようになる．

$$W = \int_\gamma P(x,y)dx + Q(x,y)dy. \tag{5.1.4}$$

$P(x,y), Q(x,y)$ を実数値関数とするとき，$P(x,y)dx + Q(x,y)dy$ の形の表現を**第 1 次微分形式**と呼ぶ．

$f(x,y)$ を 1 階の偏導関数をもつ実数値関数とするとき，その**全微分**とは次のようなものであった．

$$df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy. \tag{5.1.5}$$

この定義に従えば，2 変数関数の全微分は第 1 次微分形式である．γ が始点 P_0，終点 P_1 の曲線とすれば，定義に代入することによって

$$\int_\gamma df = f(P_1) - f(P_0).$$

すなわち，全微分の線積分は端点にのみ依存する．このとき，$\int_\gamma df$ は**経路に独立**であるという．この概念はまた後で考察するであろう．

一般に，第 1 次の微分形式 $Pdx + Qdy$ はある関数 $f(x, y)$ の全微分になっているとき**完全**であるという．このとき，$P(x, y) = \dfrac{\partial f}{\partial x}, Q(x, y) = \dfrac{\partial f}{\partial y}$ である．さらに，P, Q が連続であれば

$$\frac{\partial P}{\partial y} = \frac{\partial^2 f}{\partial x \partial y} = \frac{\partial^2 f}{\partial y \partial x} = \frac{\partial Q}{\partial x}.$$

この条件は完全性に対する十分条件であることもわかる．

補題 5.1.2 $P(x, y), Q(x, y)$ が連続であるとすれば，微分形式 $Pdx + Qdy$ が完全であるための必要十分条件は $\dfrac{\partial P}{\partial y} = \dfrac{\partial Q}{\partial x}$ なることである．

次の例は $Pdx + Qdy$ が完全であるとき，$df = Pdx + Qdy$ を満たす関数 $f(x, y)$ をいかにして決定するかという方法を示している．補題 5.1.2 の形式的な証明はこの方法に基づいている．

例 5.1.4 微分形式 $(x^3 + 3x^2 y)dx + (x^3 + y^3)dy$ が完全であることを示し，これを全微分としてもつ関数 $f(x, y)$ を決定せよ．

$P(x, y) = (x^3 + 3x^2 y), Q(x, y) = (x^3 + y^3)$ とおけば，$\dfrac{\partial P}{\partial y} = 3x^2, \dfrac{\partial Q}{\partial x} = 3x^2.$ したがって，$\dfrac{\partial P}{\partial y} = \dfrac{\partial Q}{\partial x}$ であるから，与えられた式は補題 5.1.2 より完全第 1 次微分形式である．

$$df = Pdx + Qdy = (x^3 + 3x^2 y)dx + (x^3 + y^3)dy = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy$$

と仮定する．このとき，

$$\frac{\partial f}{\partial x} = (x^3 + 3x^2 y), \quad \frac{\partial f}{\partial y} = (x^3 + y^3).$$

はじめに，$\dfrac{\partial f}{\partial x} = (x^3 + 3x^2 y)$ を x に関して積分すると

$$\int (x^3 + 3x^2 y)dx = \frac{x^4}{4} + x^3 y + g(y).$$

したがって，$f(x) = \dfrac{x^4}{4} + x^3y + g(y)$. ここで，$g(y)$ は y だけの関数である．

この式を y について微分すると $\dfrac{\partial f}{\partial y} = x^3 + g'(y) = Q(x,y) = x^3 + y^3$. これより，$g'(y) = y^3$. ゆえに，$g(y) = \dfrac{y^4}{4} + c$. これらを上式に代入すると，最終的に次を得る．

$$f(x,y) = \frac{x^4}{4} + x^3y + y^4/4 + c. \qquad \square$$

次に，グリーンの定理を考察する．この定理は 2 変数関数に対する 2 つの形の積分 (2 重積分と線積分) の間の関係を表現している 1 つの結果として考えることができる．この本の範囲外ではあるが，さらに一般的に任意の次元 (変数の数) において，同様な 2 つの形の積分とグリーンの定理に相当するものが成り立つ．

定義 5.1.2 曲線 $\gamma(t) : [a,b] \to \mathbb{C}$ が $\gamma(a) = \gamma(b)$ でかつ他の任意の対 $t_1, t_2 \in [a,b]$ に対して $\gamma(t_1) \neq \gamma(t_2)$ を満たすとき，**単純閉曲線**という．このような曲線は基本的には，共有点がそれらの端点しかない 2 つの曲線の和集合である．すなわち，自分自身と共有点がただ 1 つであり，その点は定義域の区間の端点で起こる (図 5.2 参照).

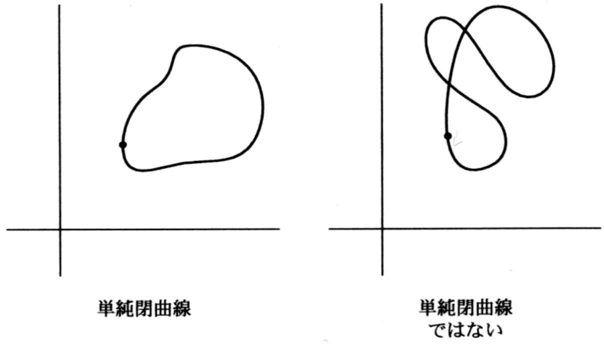


図 5.2 閉曲線

ジョルダンの曲線定理によれば単純閉曲線は平面を 2 つの集合，内部と外部とに分割する．この明らかに見える事実は，証明しようとすると驚くほど難しい．

定理 5.1.1 （グリーンの定理）

R を $\mathbb{C}$ の部分集合とし，その境界 ∂R は単純閉曲線とする．さらに，$P(x,y)$ と $Q(x,y)$ は R と ∂R を含んでいる領域 U 上で連続的微分可能であると仮定する．そのとき，次の式が成り立つ．

$$\oint_{\partial R} Pdx + Qdy = \int\int_R \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dA.$$

ここで，線積分は反時計回りに境界 ∂R に沿うものとする．

グリーンの定理はその境界が 1 つの単純閉曲線である集合よりもっと一般的な集合上に拡張できる．たとえば，G をその境界 ∂G が有限個の単純閉曲線からなり，どの 2 つも交差していないような集合とするとき，それでもグリーンの定理は成り立つ．

$$\oint_{\partial G} Pdx + Qdy = \int\int_R \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dA.$$

ここで，その境界上の線積分はそれぞれの境界曲線上の和として定義され，またそれぞれの向きは領域 G がその左側になるように定義されているものとする．

例 5.1.5 グリーンの定理は図 5.3 における集合 R に適用される．ここで，線積分は外側の境界線の回りは反時計回りで，内側の境界線は時計回りである．

□

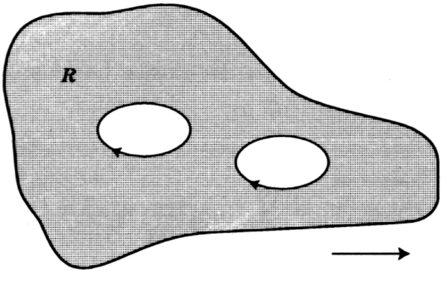


図 5.3　グリーンの定理が適用できる集合

R が長方形である場合にグリーンの定理を証明し，1 つの例を与える．

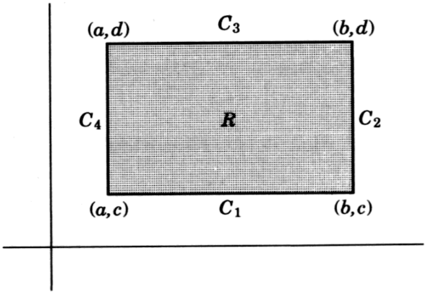


図 5.4　長方形領域

（**証明**）R を $a \leq x \leq b,\ c \leq x \leq d$ なる長方形とする．これは図 5.4 のように描かれる．

別々に，次の 2 つの式を示す．

$$\oint_{\partial R} P(x,y)dx = -\int\int_R \frac{\partial P}{\partial y}dA,$$
$$\oint_{\partial R} Q(x,y)dy = \int\int_R \frac{\partial Q}{\partial x}dA.$$

最初に，次の積分を考察する．

$$\int\int_R \frac{\partial P}{\partial y}dA = \int_a^b \int_c^d \frac{\partial P}{\partial y}dydx = \int_a^b (P(x,d) - P(x,c))dx.$$

もとの積分にもどって，

$$\oint_{\partial R} P(x,y)dx = \int_{C_1} P(x,y)dx + \int_{C_2} P(x,y)dx + \int_{C_3} P(x,y)dx + \int_{C_4} P(x,y)dx.$$

ここで，C_1 は (a,c) から (b,c) への辺，C_2 は (b,c) から (b,d) への辺，C_3 は (b,d) から (a,d) への辺，C_4 は (a,d) から (a,c) への辺を表す．

さて，C_2 と C_4 上では $dx = 0$ であり，他方 C_1 上では $y = c$, C_3 上では

$y = d$. したがって,

$$\begin{aligned}\oint_{\partial R} P(x,y)dx &= \int_{C_1} P(x,y)dx + \int_{C_3} P(x,y)dx \\ &= \int_a^b P(x,c)dx + \int_b^a P(x,d)dx = \int_a^b (P(x,c) - P(x,d))dx \\ &= -\int_a^b (P(x,d) - P(x,c))dx = \int\int_R \frac{\partial P}{\partial y} dA.\end{aligned}$$

同様にして次を得る.

$$\oint_{\partial R} Q(x,y)dy = \int\int_R \frac{\partial Q}{\partial x} dA.$$

■

一般的なグリーンの定理の証明は領域を長方形の格子に分割することによってなされる.

例 5.1.6 $P(x,y) = 4y, Q(x,y) = 5x$ とし, 集合 R を原点を中心とする半径 1 の円周を境界とする円周と円の内部とする. ∂R は $\gamma(t) = e^{it} = \cos t + i \sin t$, $0 \le t \le 2\pi$ によって表される.

$\dfrac{\partial Q}{\partial x} = 5, \dfrac{\partial P}{\partial y} = 4$ であるから, $\dfrac{\partial Q}{\partial x} - \dfrac{\partial P}{\partial y} = 1$. したがって,

$$\int\int_R \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dA = \int\int_R dA = \text{面積 } (R) = \pi.$$

さて, ∂R は単位円であるから, $x(t) = \cos t, dx = -\sin t dt, y(t) = \sin t, dy = \cos t dt$ である. 以上より,

$$\begin{aligned}\oint_{\partial R} Pdx + Qdy &= \int_0^{2\pi} 4\sin t(-\sin t)dt + 5\cos t \cos t dt \\ &= \int_0^{2\pi} (5\cos^2 t - 4\sin^2 t)dt = \int_0^{2\pi} (5 - 9\sin^2 t)dt = \pi.\end{aligned}$$

□

グリーンの定理と微分形式の完全性は経路の独立性の概念と密接に関係している. このことは複素積分においても基本的な役割を果たす.

定義 5.1.3 $P(x,y), Q(x,y)$ を曲線を含んでいる領域上で定義された関数とする．そのとき，$\int_\gamma Pdx + Qdy$ はその積分の値が曲線自身ではなく，γ の端点によってのみ決まるとき，**経路に独立**であるという．

定理 5.1.2 $P(x,y), Q(x,y)$ を領域 U 上で連続的微分可能であると仮定する．そのとき，次の命題は同値である．

(1) $P(x,y)dx + Q(x,y)dy$ は完全である．

(2) U に含まれる任意の曲線 γ に対して，$\int_\gamma Pdx + Qdy$ は経路に独立である．

(3) U に含まれる任意の単純閉曲線 γ に対して，$\int_\gamma Pdx + Qdy = 0$.

（**証明**）$P(x,y)dx + Q(x,y)dy$ は完全であると仮定する．そのとき，$df = Pdx + Qdy$ を満たす関数 $f(x,y)$ が存在する．P_0, P_1 を U の 2 つの点とし，γ を端点が P_0, P_1 である U 内の任意の曲線とする．すると，

$$\int_\gamma Pdx + Qdy = \int_\gamma df = f(P_1) - f(P_0).$$

したがって，$\int_\gamma Pdx + Qdy$ は経路に独立である．よって，(1) から (2) が示された．

U に含まれる任意の曲線 γ に対して，$\int_\gamma Pdx + Qdy$ は経路に独立であると仮定する．γ_1 を単純閉曲線とする．P_0, P_1 を γ_1 上の 2 つの点とする．図 5.5 で示したように，γ_{11} を γ_1 に沿って P_0 から P_1 へ向かう曲線，γ_{12} を γ_1 に沿って P_0 から P_1 へ向かう曲線とする．

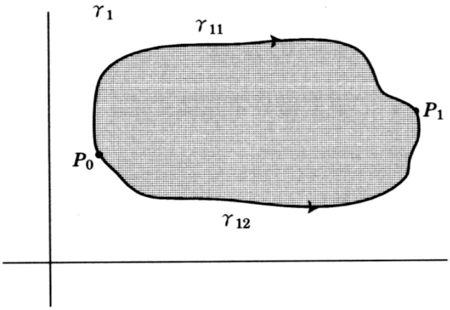


図 5.5 経路の独立性

経路の独立性より，

$$\int_{\gamma_{11}} Pdx + Qdy = \int_{\gamma_{12}} Pdx + Qdy$$

すなわち，

$$\int_{\gamma_{11}} Pdx + Qdy - \int_{\gamma_{12}} Pdx + Qdy = 0.$$

一方，元の曲線 γ_1 は $\gamma_{11} - \gamma_{12}$ であるから，

$$\int_{\gamma_1} Pdx + Qdy = \int_{\gamma_{11}} Pdx + Qdy - \int_{\gamma_{12}} Pdx + Qdy = 0.$$

したがって，(2) ならば (3) が示された．

最後に，U に含まれる任意の単純閉曲線 γ に対して，$\int_\gamma Pdx + Qdy = 0$ と仮定する．

グリーンの定理より，

$$\int\int_{\gamma\text{の内部}} \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right) dA = 0.$$

この式は任意の単純閉曲線に対して成り立つので，U における任意の単純閉曲線によって囲まれている U の任意の領域に対して成り立つ．ところが，これが成り立つのは次の場合に限る．

$$\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} = 0 \quad \text{すなわち} \quad \frac{\partial Q}{\partial x} = \frac{\partial P}{\partial y}.$$

したがって，$Pdx + Qdy$ は完全である．以上によって，定理の証明は完結した．■

5.2　複素積分とコーシーの定理

実線積分の理論を用いて複素積分を定義する．

定義 5.2.1

(a) $f(t) = u(t) + iv(t)$ を区間 $t_0 \le t \le t_1$ 上で定義された連続な複素関数とする．このとき，次のように定義する．

$$\int_{t_0}^{t_1} f(t)dt = \int_{t_0}^{t_1} u(t)dt + i\int_{t_0}^{t_1} v(t)dt. \qquad (5.2.1)$$

(b) $f(z) = u(z)+iv(z)$ を連続な複素関数とし，$\gamma(t) = x(t)+iy(t), t_0 \le t \le t_1$ は $\gamma(t)$ が $f(z)$ の定義域の中にある曲線とする．このとき，$f(\gamma(t))$ は実変数 t の連続な複素関数である．次の式によって，**周回積分**あるいは**複素線積分**を定義する．

$$\int_\gamma f(z)dz = \int_{t_0}^{t_1} f(\gamma(t))\gamma'(t)dt. \tag{5.2.2}$$

この複素線積分の定義は次の意味において，曲線の媒介変数表示には無関係である．2 つの曲線を $\gamma_1 : [t_0, t_1] \to \mathbb{C}, t_0 \le t_1$，$\gamma_2 : [s_0, s_1] \to \mathbb{C}, s_0 \le s_1$ とする．連続的微分可能な全単射である関数 $\phi : [t_0, t_1] \to [s_0, s_1]$ が存在して，$\gamma_2 = \gamma_1 \circ \phi$, $\phi'(t) > 0$(任意の $t \in [t_0, t_1]$ に対して) を満たすとき，γ_1 と γ_2 は**同値**であるという．さて，γ_1 と γ_2 をある開集合 $U \subset \mathbb{C}$ に値をとる同値な曲線とし，$f(z)$ は U で連続であるとする．このとき，$\gamma_2'(t) = \gamma_1'(\phi(t))\phi'(t)$ であるから次の式が成り立つ．

$$\int_{\gamma_1} f(z)dz = \int_{\gamma_2} f(z)dz.$$

$f(z) = u(z)+iv(z), \gamma(t) = x(t)+iy(t)$ と表せば，$\gamma'(t)dt = x'(t)dt+iy'(t)dt = dx + idy = dz$. これらを，代入すると

$$f(z)dz = (u + iv)(dx + idy) = udx - vdy + i(udy + vdx).$$

したがって，複素線積分の定義は次のように書き換えることができる．

$$\int_\gamma f(z)dz = \int_\gamma (udx - vdy) + i \int_\gamma (vdx + udy). \tag{5.2.3}$$

例 5.2.1 γ を始点 (0,0)，終点を (1,1) とする線分とするとき，$\int_\gamma z^3 dz$ を計算せよ．

$z^3 = (x + iy)^3 = x^3 - 3xy^2 + i(3x^2y - y^3)$ であり，一方 (0,0) から (1,1) へ

の線分は $\gamma(t) = t + it, 0 \leq t \leq 1$ によって表される．したがって，

$$\begin{aligned}\int_\gamma f(z)dz &= \int_\gamma (udx - vdy) + i\int_\gamma (vdx + udy)\\ &= \int_\gamma (x^3 - 3xy^2)dx - (3x^2y - y^3)dy\\ &\quad + i\int_\gamma (3x^2y - y^3)dx + (x^3 - 3xy^2)dy\\ &= \int_0^1 (t^3 - 3t^3)dt - (3t^3 - t^3)dt\\ &\quad + i\int_0^1 (3t^3 - t^3)dt + (t^3 - 3t^3)dt\\ &= \int_0^1 (-4t^3)dt = -1.\end{aligned}$$

□

この線積分についての基本的な結果より，すべての標準的な積分の性質が複素積分においても成り立つことがわかる．

補題 5.2.1 $f(z), g(z)$ を連続な複素関数とし，$\alpha, \beta \in \mathbb{C}$ とする．このとき，次が成り立つ．

(1) $\displaystyle\int_\gamma \alpha f(z) + \beta g(z)dz = \alpha\int_\gamma f(z)dz + \beta\int_\gamma g(z)dz.$

(2) $\displaystyle|\int_\gamma f(z)dz| \leq \int_\gamma |f(z)||dz|.$

(3) $\displaystyle\int_\gamma |dz| = \gamma$ の弧長.

(4) γ 上で $|f(z)| \leq M$ であり，γ の弧長を L とすると，$\displaystyle|\int_\gamma f(z)dz| \leq ML.$

$F(z) = U(z) + iV(z)$ が曲線 γ を含んでいるある領域上で解析的であり，さらに $f(z) = F'(z)$ と仮定する．そのとき，$f(z) = \dfrac{\partial U}{\partial x} + i\dfrac{\partial V}{\partial x}$ であり，(5.2.3) 式より次が得られる．

$$\int_\gamma f(z)dz = \int_\gamma \left(\frac{\partial U}{\partial x}dx - \frac{\partial V}{\partial x}dy\right) + i\int_\gamma \left(\frac{\partial V}{\partial x}dx + \frac{\partial U}{\partial x}dy\right). \tag{5.2.4}$$

コーシー・リーマンの微分方程式より，$\dfrac{\partial U}{\partial x} = \dfrac{\partial V}{\partial y}, \dfrac{\partial U}{\partial y} = -\dfrac{\partial V}{\partial x}$ である．ゆえに，

$$\frac{\partial^2 U}{\partial x\partial y} = \frac{\partial^2 U}{\partial y\partial x} = -\frac{\partial^2 V}{\partial x^2} \quad \text{かつ} \quad \frac{\partial^2 V}{\partial x\partial y} = \frac{\partial^2 V}{\partial y\partial x} = \frac{\partial^2 U}{\partial x^2}.$$

ここで (5.2.4) 式の右辺の 2 つの積分は経路には独立である．したがって，曲線 γ が z_0 から z_1 へ向かうとき，このことは次のことを意味している．

$$\int_\gamma f(z)dz = \int_\gamma F'(z)dz = F(z_1) - F(z_0). \tag{5.2.5}$$

これは，微積分学の基本定理の複素版である．

補題 5.2.2 $F(z)$ が領域 U 上で解析的であり，$f(z) = F'(z)$ と仮定する．U に含まれる任意の曲線を γ とし，その端点を z_0, z_1 とする．このとき，次が成り立つ．

$$\int_\gamma f(z)dz = F(z_1) - F(z_0).$$

系 5.2.1 任意の自然数 n と端点を z_0, z_1 とする任意の曲線 γ に対して，

$$\int_\gamma z^n dz = \left[\frac{z^{n+1}}{n+1}\right]_{z_0}^{z_1} = \frac{z_1^{n+1}}{n+1} - \frac{z_0^{n+1}}{n+1}$$

が成り立つ．

例 5.2.2 γ を始点 $(0,0)$，終点を $(1,1)$ とする線分とするとき，$\int_\gamma z^3 dz$ を計算せよ．

ここで，γ の端点は 0 と $1+i$ であるから，系 5.2.1 を使うと

$$\int_\gamma z^3 dz = \left[\frac{z^4}{4}\right]_0^{1+i} = \frac{(1+i)^4}{4} = -1.$$

この結果は例 5.2.1 において直接計算したものと同じであることに注意せよ．

補題 5.2.2 の直接の結果として，閉曲線 γ に対して次が成り立つ．

$$\int_\gamma F'(z)dz = 0.$$

この結果を解析的な被積分関数に拡張する．$f(z)$ が曲線 γ を含んでいるある集合 U 上で解析的であるとき，次の積分を考える．

$$\int_\gamma f(z)dz = \int_\gamma (udx - vdy) + i\int_\gamma (vdx + udy).$$

コーシー・リーマンの微分方程式より，

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

ゆえに，これらの偏導関数が U で連続であるとするとき，上の積分の式における各微分形式は完全である．したがって，線積分は経路に独立である．以上によって，U に含まれている任意の閉曲線 γ に対して次の式が成り立つ．

$$\int_\gamma f(z)dz = 0. \tag{5.2.6}$$

この結果ははじめ 1800 年代の初期にコーシーによって与えられた．同世紀の後期にグールサが，$f(z)$ の解析性だけで十分であることを証明した (その証明は偏導関数の連続性によるものではなく，したがって，グリーンの定理から得られるものよりも強い証明である)．このような理由でこの結果は**コーシーの定理**または**コーシー・グールサの定理**と名付けられている．付録 B において，拡張されたグールサの定理の正式な証明を与える．　□

定理 5.2.1（コーシーの定理）$f(z)$ を単連結領域 U 上で解析的であり，γ を U に含まれている閉曲線とする．このとき，次が成り立つ．

$$\int_\gamma f(z)dz = 0.$$

コーシーの定理は，すべての解析関数はそれ自身ある解析関数の導関数であることを含んでいる，ということを証明してこの節を終えることにしよう．

定理 5.2.2 $f(z)$ を単連結領域 U 上の解析関数とするとき，U で解析的な関数 $F(z)$ が存在して $f(z) = F'(z)$ を満たす．

（証明） z_0 を U の固定した点とする．始点を z_0 とする U の任意の曲線 γ に対して，コーシーの定理より積分 $\int_\gamma f(z)dz$ の値は γ の終点にのみ依存することがわかる．これを確かめるために，図 5.6 のように z_0 を始点をとし，z_1 で終わる 2 つの曲線を γ, γ_1 とする．

γ_2 を γ に沿って z_0 を出発し，γ_1 に沿って z_0 にもどる閉曲線とする．$f(z)$ は U 上で解析的であるから，コーシーの定理より

$$\int_{\gamma_2} f(z)dz = 0 = \int_\gamma f(z)dz - \int_{\gamma_1} f(z)dz.$$

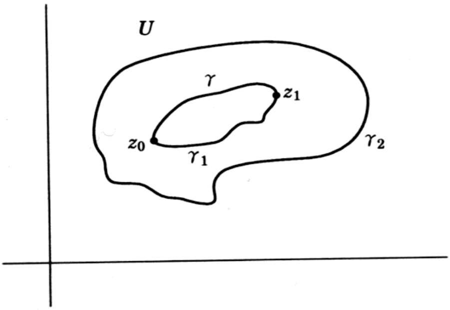


図 5.6　経路の独立性

ゆえに，

$$\int_{\gamma} f(z)dz = \int_{\gamma_1} f(z)dz.$$

ここで，$F(z) = \int_{z_0}^{z_1} f(w)dw$ とおく．上の議論より，これは矛盾なく定義されている．そこで，$F'(z) = f(z)$ を証明する．

$$F'(z) = \lim_{\Delta z \to 0} \frac{F(z+\Delta z) - F(z)}{\Delta z} = \lim_{\Delta z \to 0} \frac{1}{\Delta z}\left(\int_{z_0}^{z+\Delta z} f(w)dw - \int_{z_0}^{z} f(w)dw\right)$$
$$= \lim_{\Delta z \to 0} \frac{1}{\Delta z} \int_{z}^{z+\Delta z} f(w)dw.$$

$f(z)$ は解析的であるから，連続であって，次の式が成り立つことが示される（演習問題参照）．

$$\int_{z}^{z+\Delta z} f(w)dw = (f(z) + \epsilon)\Delta z,$$

ここで，$\Delta z \to 0$ のとき，$\epsilon \to 0$ である．

したがって，

$$\lim_{\Delta z \to 0} \frac{1}{\Delta z} \int_{z}^{z+\Delta z} f(w)dw = f(z).$$

以上より，$F'(z) = f(z)$ を得る．■

5.3　コーシーの積分公式とコーシーの評価式

コーシーの定理を用いて，**コーシーの積分公式**として知られている次の基本的な結果を証明する．

定理 5.3.1（コーシーの積分公式）$f(z)$ を単純閉曲線 γ を含んでいる単連結領域 U において解析的な関数とする．z_0 を γ の任意の内部の点[2] とすれば，次の式が成り立つ．

$$f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z - z_0}dz.$$

ここで，積分路は γ に沿って反時計回りにとるものとする．

定理の証明を与える前に，この定理は次のことを主張していることに注意しよう．すなわち，U において解析的な関数の，U 内の閉曲線 γ の内側における値は γ の境界線上の値によって完全に決定される．したがって，解析性はこのような曲線の境界線上の値と内部の点における値との間にこのような非常に強い関係を要請している．

（証明）(定理 5.3.1) C_0 を z_0 を中心として，半径 r_0 の円とする．r_0 が十分小さければ，図 5.7 のように，C_0 は γ の内部に含まれる．

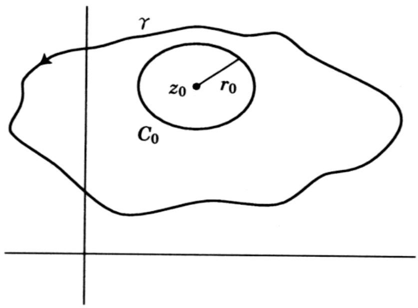


図 5.7　曲線で囲まれた領域

そのとき，関数 $g(z) = \dfrac{f(z)}{z - z_0}$ は曲線 γ と C_0 円によってはさまれた環の形の領域上で解析的である．したがって，コーシーの定理により

$$\int_\gamma \frac{f(z)}{z - z_0}dz - \int_{C_0} \frac{f(z)}{z - z_0}dz = 0. \tag{5.3.1}$$

ゆえに，

$$\int_\gamma \frac{f(z)}{z - z_0}dz = \int_{C_0} \frac{f(z)}{z - z_0}dz.$$

[2] 内点のこと，境界は含まない．定義 8.3.7 を参照せよ (p.170).

このとき，

$$\int_\gamma \frac{f(z)}{z-z_0}dz = f(z_0)\int_{C_0}\frac{dz}{z-z_0}dz + \int_{C_0}\frac{f(z)-f(z_0)}{z-z_0}dz. \tag{5.3.2}$$

さて，C_0 上では $z = z_0 + r_0e^{it}$ かつ $dz = ir_0e^{it}dt$ であるから

$$\int_{C_0}\frac{dz}{z-z_0} = i\int_0^{2\pi} dt = 2\pi i.$$

$f(z)$ は z_0 で連続であるから，r_0 を十分小さく選んでおけば $|z-z_0| \leq r_0$ (C_0 の内部) である限り $|f(z)-f(z_0)| < \epsilon$ となっている．そのとき，

$$\left|\int_{C_0}\frac{f(z)-f(z_0)}{z-z_0}dz\right| \leq \int_{C_0}\frac{|f(z)-f(z_0)|}{|z-z_0|}|dz| < \frac{\epsilon}{r_0}2\pi r_0 = 2\pi\epsilon.$$

したがって，式 (5.3.2) の右辺第 2 項の積分の絶対値は任意に小さくすることができる．それゆえ，その値は 0 でなければならない．ゆえに，

$$\int_\gamma \frac{f(z)}{z-z_0}dz = 2\pi i f(z_0).$$

■

例 5.3.1 その内部に $z=3$ を含み，$z=-3$ を含まない任意の単純閉曲線を γ とする．このとき，積分 $\displaystyle\int_\gamma \frac{dz}{z^2-9}$ を計算せよ．

$f(z) = \dfrac{1}{z+3}$ とおく．γ はその内部に $z=-3$ を含まなければ，$f(z)$ は γ 上とその内部で解析的である．したがって，コーシーの積分公式によって

$$\int_\gamma \frac{dz}{z^2-9} = \int_\gamma \frac{dz}{(z+3)(z-3)} = \int_\gamma \frac{f(z)}{z-3}dz = 2\pi i f(3).$$

ゆえに，この値は $2\pi i/6$ である．

高等微積分学において次のことを学んだ．$g(x,t)$ を微分可能な 2 変数関数として，

$$f(t) = \int_a^b g(x,t)dt$$

とおくと，次が成り立つ．

$$f'(t) = \int_a^b \frac{\partial g}{\partial t}(x,t)dt.$$

すなわち，ある関数が微分可能な2変数関数を1つの変数について積分することによって定義されているとすれば，その導関数はその変数に関する偏導関数を積分したものになっている．

さて，この考えをコーシーの積分公式に適用して解析関数の導関数に対する1つの表現を得る．

$$f(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z - z_0}dz.$$

z_0 に関して，この積分の内側を微分して，つぎの式を得る．

$$f'(z_0) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{(z - z_0)^2}dz. \tag{5.3.3}$$

帰納的に，z_0 に関してこれを微分することができて次の公式を得る．

$$f^{(n)}(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z - z_0)^{n+1}}dz. \tag{5.3.4}$$

□

以上によって，コーシーの積分公式から得られる次の系を証明したことになる．

系 5.3.1　$f(z)$ を単純閉曲線 γ を含んでいる単連結領域 U において解析的な関数とする．z_0 を γ の内部の任意の点とすれば，第 n 階の導関数は次の式によって与えられる．

$$f^n(z_0) = \frac{n!}{2\pi i}\int_\gamma \frac{f(z)}{(z - z_0)^{n+1}}dz.$$

特に，このことは $f(z)$ がある集合 U 上で解析的ならば，それは U においてすべての階数の導関数をもつことを示している．

系 5.3.2　$f(z)$ が単連結領域 U 上で解析的ならば，それは U においてすべての階数の導関数をもつ．

解析関数は他のもう1つの解析関数の導関数となっていることを思い出そう．系 5.3.2 の結果として，解析関数の導関数は再び解析関数であることがわかる．

系 5.3.3 解析関数の導関数はそれ自身解析関数である．

ここで，$\mathbb{R}$ 上の実数値関数と比較してみよう．関数 $y = f(x), x, y \in \mathbb{R}$ は 1 回は微分可能であっても，2 回微分可能でないこともあり得る．一般に，関数 $f : [a, b] \to \mathbb{R}$ は n 回連続微分可能であるとき，C^n 級であるという．各 n に対して，C^{n+1} は，C^n の真部分集合である．すなわち，n 回連続微分可能ではあるが $n+1$ 回は連続微分可能でない関数が存在する．

C^∞ は無限回微分可能な関数からなる集合である．たとえば，e^x と $\sin x$ はそのような関数である．系 5.3.2 は次のことを主張している．複素関数にとって，ある集合上で解析的ならば，その集合上で C^∞ 級であることを意味している．

実解析関数とは収束するテイラー級数によって表される関数のことである．明らかに，このような関数は C^∞ 級である．しかしながら，実解析的ではない C^∞ 級の関数も存在する．このようなことは，複素関数の場合では起こらない．ある集合上で解析的ならば，その集合上でテイラー級数に展開できることを意味している．

定理 5.3.2 $f(z)$ を z_0 を中心として，半径 r_0 の円 C_0 の内部において解析的とする．そのとき，円 C_0 の内部において $f(z)$ は z_0 に中心をもつ収束するテイラー級数によって表現される．すなわち，C_0 の内部のすべての点 z に対して，

$$f(z) = f(z_0) + f'(z_0)(z - z_0) + \cdots + \frac{(f^{n+1})}{n!}(z - z_0)^n + \cdots.$$

最後に，コーシーの積分公式から**コーシーの評価式**が得られる．これは代数学の基本定理の第 2 の証明において道具となるものである．

定理 5.3.3（コーシーの評価式）$f(z)$ を z_0 を中心として，半径 r_0 の円 C_0 を含んでいる単連結領域 U において解析的とする．M を C_0 上での $|f(z)|$ の最大値とすれば，次の不等式が成り立つ．

$$|f^{(n)}(z_0)| \leq \frac{n!M}{r_0^n}.$$

特に，C_0 上とその内部で $|f(z)| < M$ ならば，C_0 の内部の任意の点 z に対して次が成り立つ．

$$|f'(z)| < \frac{M}{r_0}.$$

（証明） 系 5.3.1 より，

$$|f^{(n)}(z_0)| \leq \left| \frac{n!}{2\pi i} \int_{C_0} \frac{f(z)}{(z-z_0)^{n+1}} dz \right| \leq \frac{Mn!}{2\pi} \left| \int_{C_0} \frac{dz}{(z-z_0)^{n+1}} \right|.$$

C_0 上で，$z = z_0 + r_0 e^{it}$，$dz = ir_0 e^{it} dt$ であるから

$$\left| \int_{C_0} \frac{dz}{(z-z_0)^{n+1}} \right| = \left| \int_0^{2\pi} r_0^{-n} e^{-int} dt \right| = 2\pi r_0^{-n}.$$

ゆえに，$|f^{(n)}(z_0)| \leq \dfrac{Mn!}{r_0^n}$ を得る． ■

5.4　リウヴィルの定理と代数学の基本定理——証明 2

コーシーの評価式に基づいて**リウヴィルの定理**を証明することができる．そしてこのリウヴィルの定理より，代数学の基本定理の第 2 の証明が容易に得られる．

定理 5.4.1（リウヴィルの定理）

(1) $f(z)$ が整関数でかつ全複素平面上で有界であるならば，$f(z)$ は定数である．

(2) 一般的には，$|f^{(n)}(z)|$ が $\mathbb{C}$ 上で有界ならば，$f(z)$ は次数が高々 $n+1$ の多項式である．

（証明） (1) $f(z)$ が整関数で，すべての $z \in \mathbb{C}$ に対して $|f(z)| \leq M$ と仮定する．そのとき，原点を中心として半径 r の円上でのコーシーの評価式より，

$$|f'(z)| < \frac{M}{r}.$$

$f(z)$ は整関数であるから，$r \to \infty$ とすることができる．ゆえに，$|f'(z)| = 0$．したがって，$f'(z) = 0$ である．もちろん，これは $f(z)$ が定数であることを意味しているので，(1) が証明された．

(2) $|f^n(z)| \leq M$ $(\forall z \in \mathbb{C})$ と仮定すれば，再び原点を中心として半径 r の円上でのコーシーの評価式より，

$$|f^{n+1}(z)| \leq \frac{M}{r}.$$

同様にして，$r \to \infty$ とすれば $f^{n+1}(z) = 0$ が得られ，$f^n(z)$ は定数となる．そのとき，微分と逆の操作によって $f(z)$ は次数が高々 $n+1$ の多項式となる．

■

$P(z)$ を複素多項式と仮定する．$\deg P(z) \geq 1$ ならば，$P(z)$ は $|P(z)| \to \infty$ $(|z| \to \infty)$ なる性質をもつ定数でない整関数である．これらの事実をリウヴィルの定理と結びつけると代数学の基本定理の証明が得られる．

定理 5.4.2（代数学の基本定理）$P(z)$ を次数が 1 以上の複素多項式とする．このとき，$P(z)$ は少なくとも 1 つの複素数の根をもつ．

（証明） $P(z)$ を複素多項式として，$f(z) = \dfrac{1}{P(z)}$ とおく．$P(z)$ が複素数の根をもたなければ，$f(z)$ も整関数となる．

$|z| \to \infty$ のとき $|P(z)| \to \infty$ であるから，ある正の数 M, r が存在して，$|z| > r$ に対して $|P(z)| > M$ が成り立つ．これは $|z| > r$ のとき，$|f(z)| = \dfrac{1}{|P(z)|} < \dfrac{1}{M}$ を意味している．$f(z)$ が整関数であれば，それは連続関数であるから $|z| \leq r$ なるコンパクト集合上で有界である．したがって，$f(z)$ が整関数ならば，それは $\mathbb{C}$ 上で有界である．そのときリウヴィルの定理によって，$f(z)$ は定数である．よって $P(z)$ も定数となるが，これは矛盾である．以上により，$f(z)$ は少なくとも 1 つの $z \in \mathbb{C}$ において 0 とならなければならない．

■

ここで証明したことは，実際は次のようなことである．$|z| \to \infty$ のとき $|f(z)| \to \infty$ なる性質をもつ定数でない整関数 $f(z)$ は少なくとも 1 つのゼロ点を $\mathbb{C}$ にもつ．すなわち，$f(z_0) = 0$ を満たす点 $z_0 \in \mathbb{C}$ が存在する．しかしながら，注意深く整関数を考察するならば，このような関数は多項式であることがわかる．特に，多項式は無限遠点において無限大である整関数として特徴づけられる．この方面の考察に対して興味のある読者はアールフォースの文献 [A] を参照せよ．

5.5　いくつかの付加的な結果

この章を 2 つの付加的な結果を証明することによって閉じることにしよう．これらの結果は代数学の基本定理に直接関係のあるものではないが，リウヴィルの定理などと同じ一連の一般的な発展的成果のなかの 1 部である．

その最初のものは**モレラの定理**と呼ばれており，これはコーシーの定理の部分的な逆を与えるものである．特に，連続関数が適当な集合の中にあるすべての単純閉曲線上での積分がゼロであれば，それは解析関数である，ということを主張している．

定理 5.5.1（モレラの定理）$f(z)$ が単連結領域 U 上で連続で，U の内部にあるすべての単純閉曲線 γ に対して $\int_\gamma f(z)dz = 0$ と仮定する．そのとき，$f(z)$ は U 上で解析的である．

（証明） 証明は本質的に定理 5.2.2 のそれと同じである．

z_0 を U の固定した点とする．U の内部にあるすべての単純閉曲線 γ に対して $\int_\gamma f(z)dz = 0$ であるから，z_0 を始点とする任意の曲線 γ_1 に対して $\int_{\gamma_1} f(z)dz$ の値は γ_1 の終点にのみ依存する．したがって，

$$F(z) = \int_{z_0}^{z_1} f(w)dw$$

は矛盾なく定義される．定理 5.2.2 の証明と同様にして $F'(z) = f(z)$ を証明することができる．

$F(z)$ は U で微分可能であるから，解析的であり，ゆえに $f(z)$ はある解析関数の導関数である．したがって，系 5.3.3 より $f(z)$ は解析関数である．■

これから述べる第 2 の結果は**最大値定理**と呼ばれている．この定理はコンパクトな領域上の解析関数に対して，その最大値はその境界上でとるというものである．

定理 5.5.2（最大値定理）$f(z)$ が有界領域 D 上で定数ではなく，解析的であり，D の境界上で連続であると仮定する．そのとき，$|f(z)|$ は D の境界上でその最大値をとり，その内部の点では決して最大値をとらない．

（証明） 証明は次に述べるような**最大値の原理**にのみ基づいている．

$f(z)$ が領域 U において定数ではなく解析的ならば，$z_0 \in U$ の U におけるすべての近傍は $|f(z)| > |f(z_0)|$ を満たす点 z を含んでいる．

付録 C において，代数学の基本定理の別証明をするために最大値の原理を使う．

5.6　複素解析学についての結論

これまでの 2 つの章において，複素解析学における多くの考え方と技術を発展させ，それらを用いて代数学の基本定理の第 2 の証明を与えた．この発展の中の鍵となる道具は，リウヴィルの定理と代数学の基本定理の第 2 の証明へと導いた一連の結果の出発点であるコーシーの定理であった．第 5.2 節で言及したように，グールサは実際にコーシーの定理のかなり強いバージョンを証明した．付録 B において，複素解析学にもどり，コーシーの定理と最大値の原理をさらに詳しく調べる．これを使って，付録 C において代数学の基本定理のさらに 3 つの複素解析学的な証明を与える．次の 2 つの章において，代数学の基本定理の代数的証明を考察する．

演習問題

5.1　次の積分を計算せよ．

(a) $\displaystyle\int_\gamma (x^2+y)dx + (x-y^2)dy$. ただし，$\gamma$ は $(0,0)$ から $(2,3)$ へ向かう線分である．

(b) $\displaystyle\int_\gamma (x^2-2y)dx + (2x+y^2)dy$. ただし，$\gamma$ は $(\frac{1}{2},1)$ から $(\frac{3}{4},2)$ へ向かう曲線 $y^2 = 4x-1$ である．

(c) $\displaystyle\int_\gamma \sqrt{x+(3y)^{\frac{5}{3}}}\,ds$. ただし，$\gamma$ は $x=0$ から $x=3$ へ向かう曲線 $y = \dfrac{1}{3}x^3$ である．

(d) $\displaystyle\int_\gamma (x^2+y^2)dx + (x^2-y^2)dy$. ただし，$\gamma$ は曲線 $\gamma : x(t) = t^2+3, y(t) = t-1, 1 \le t \le 2$.

(e) $\displaystyle\int_\gamma \frac{ydx+xdy}{\sqrt{x^2+y^2}}$. ただし，$\gamma$ は閉曲線 $\gamma : x = \cos t, y = \sin t, 0 \le t \le 2\pi$.

5.2 次の被積分関数は完全 1 次微分形式であることを示し，適当な不定積分を見つけて積分せよ．

(a) $\int_\gamma (x^2+2y)dx+(2x+y^2)dy$. ただし，$\gamma$ は $(1,1)$ から $(5,3)$ へ向かう曲線である．

(b) $\int_\gamma (e^x\cos y)dx-(e^x\sin y)dy$. ただし，$\gamma$ は $(0,0)$ から (π,π) へ向かう曲線である．

5.3 次のそれぞれにおいて，グリーンの定理を確かめよ．

(a) $P(x,y)=-y, Q(x,y)=x$, で，R は単位正方形の集合：$0\le x\le 1, 0\le y\le 1$.

(b) $P(x,y)=xy, Q(x,y)=-2xy$, で，R は長方形の集合：$1\le x\le 2, 0\le y\le 3$.

5.4 グリーンの定理を用いて，R が単純閉曲線 ∂R によって囲まれた領域とするとき，次の式が成り立つことを確かめよ．

$$R \text{ の面積 } = \int_{\partial R} x\,dy.$$

5.5 次の複素積分を計算せよ．

(a) $\int_\gamma f(z)dz$. ただし，$f(z)=(y-x)-3x^2 i$, γ は $z=0$ から $z=1+i$ へ向かう線分である．

(b) $\int_\gamma f(z)dz$. ただし，$f(z)=\dfrac{z+2}{z}$ で $\gamma(t)=2e^{it}$ $(0\le t\le\pi)$.

5.6 C_0 を $\gamma(t)=z_0+re^{it}$ $(0\le t\le 2\pi)$ で表される円とするとき，次の式を直接計算せよ (この式をコーシーの積分定理と比較してみよ).

$$\int_{C_0}\frac{dz}{z-z_0}=2\pi i,\quad \int_{C_0}\frac{dz}{(z-z_0)^n}=0\ \ (n=2,3,\cdots).$$

5.7 γ を反時計回りの正方形 $-2\le x\le 2, -2\le y\le 2$ の境界とする．このとき，次の積分の値は何か，またなぜか．

(a) $\displaystyle\int_\gamma \frac{e^z}{z-\pi i/2}dz$.

(b) $\displaystyle\int_\gamma \frac{z^5}{z(z^2+8)}dz$.

(c) $\displaystyle\int_\gamma \frac{z}{2z+1}dz$.

(d) $\displaystyle\int_\gamma \frac{z^4}{(z-(1+i))^2}dz$.

5.8　$f(z)$ は z_0 を内点としてもつ曲線上およびその内部で解析的であるとする．このとき，次の式が成り立つことを示せ．

$$\int_\gamma \frac{f'(z)}{z-z_0}dz = \int_\gamma \frac{f(z)}{(z-z_0)^2}dz.$$

5.9　実関数 $f(x)=e^{-\frac{1}{x^2}}$ は $x=0$ で C^∞ であるが，$x=0$ において実解析的ではないことを示せ．

第6章

体と拡大体

6.1 代数拡大

これまでに代数学の基本定理の 2 つの証明を与えた．この 2 つは，どちらの証明も代数的というよりはむしろ解析的なものであった．最初の証明は，実係数の多項式の連続性と共に高等微積分学における 2 変数実数値関数の解析的な性質に基づいている．また 2 番目の証明は複素解析学の理論を用いて証明されている．この章では，代数学の基本定理へのより代数的なアプローチを試みよう．このアプローチの言葉，代数的な言語では，結局，複素数体は**代数的閉体**である，という代数学の基本定理と同値な命題を証明することになる．

F と F' が体であって，F が F' の部分体ならば，F' は F の**拡大体**である，または単に**拡大**であるという．そのとき F' は F 上のベクトル空間であり (第 2 章参照)，F 上のベクトル空間としての F' の次元を**拡大次数**という．この拡大次数を $[F':F]$ で表す．この次数が有限ならば，すなわち，$[F':F]<\infty$ ならば，F' は F 上有限次元ベクトル空間であるが，このとき，F' は F の**有限次拡大**という．

拡大次数は乗法的であることがベクトル空間の理論より容易にわかる．具体的に表すと，次のようである．

補題 6.1.1 $F\subset F'\subset F''$ を体の拡大とし，F'' は F の有限次拡大とする．このとき，$[F':F]$ と $[F'':F']$ も有限であり，$[F'':F]=[F'':F'][F':F]$ が成

り立つ．

（**証明**）$[F' : F]$ と $[F'' : F']$ が有限であることは，部分空間の次元は全体の次元を越えないという線形代数学の理論から容易に従う．

$[F' : F] = n$ とおき，F 上 F' の基底を $\alpha_1, \cdots, \alpha_n$，また $[F'' : F'] = m$ とおき，F' 上 F'' の基底を $\beta_1, \cdots, \beta_m$ とする．このとき，mn 個の積 $\{\alpha_i \beta_j\}$ は F 上 F'' の基底をつくる（演習問題参照）．したがって，$[F'' : F] = mn = [F'' : F'][F' : F]$ が成り立つ． ■

上の補題のような場合に，F' を**中間体**といい (F と F'' の存在が前提にあるとして)，F を**基礎体**という．

例 6.1.1 $\mathbb{C}$ は $\mathbb{R}$ の有限次拡大であるが，$\mathbb{R}$ は $\mathbb{Q}$ の無限次拡大である (例 2.1.3 参照)．

我々の基本的なアプローチは，1 つの基礎体を固定した上で，その基礎体の拡大であってその要素がそれぞれ基礎体の元を係数とする，ある多項式の根となっているような拡大体を考察することである．このために，次の定義が必要である．

定義 6.1.1 F' は F の拡大体として，$\alpha \in F'$ とする．ある多項式 $0 \neq p(x) \in F[x]$ が存在して，$p(\alpha) = 0$ を満たすとき，α は F 上**代数的**であるという (α は F に係数をもつ多項式の根である)．F' のすべての元が F 上代数的であるとき，F' は F の**代数拡大**という．

$\alpha \in F'$ が F 上代数的でないとき，α は F 上**超越的**であるという．代数拡大でない拡大を**超越拡大**という．

補題 6.1.2 F のすべての元は F 上代数的である．

（**証明**）$f \in F$ に対して，$p(x) = x - f \in F[x]$ とおけば，$p(f) = 0$ である． ■

有限次拡大と代数拡大との関係は次の定理により示される．

定理 6.1.1 F' が F の有限次拡大ならば，F' は F の代数拡大である．

（**証明**）$\alpha \in F'$ とする．このとき，$p(\alpha) = 0$ を満たす 0 でない多項式 $p(x) \in F[x]$ が存在することを示さなければならない．

F' は有限次拡大であるから，$[F' : F] = n < \infty$. ゆえに，n 個の元からなる F 上のベクトル空間 F' の基底が存在する．したがって，F' の任意の $n+1$ 個の元からなる集合は F 上 1 次従属である．

$1, \alpha, \alpha^2, \cdots, \alpha^n$ なる元を考える．これら $n+1$ 個の元は F' にあるから，上に述べたことより 1 次従属である．そのとき，すべては 0 でない元 $f_0, f_1, \ldots, f_n \in F$ が存在して次の式を満たす．

$$f_0 + f_1\alpha + \cdots + f_n\alpha^n = 0. \tag{6.1.1}$$

$p(x) = f_0 + f_1 x + \cdots + f_n x^n$ とおけば，$p(x) \in F[x]$ であり，$p(\alpha) = 0$ となる．

■

例 6.1.2 $\mathbb{C}$ は $\mathbb{R}$ 上代数的であるが，$\mathbb{R}$ は $\mathbb{Q}$ 上超越的である．

$[\mathbb{C} : \mathbb{R}] = 2$ であるから，$\mathbb{C}$ が $\mathbb{R}$ 上代数的であることは定理 6.1.1 より従う．より直接に，$z \in \mathbb{C}$ とすれば $p(x) = (x - z)(x - \bar{z}) \in \mathbb{R}[x]$ であり，かつ $p(z) = 0$ である．

$\mathbb{R}$ が (したがって，$\mathbb{C}$ も) $\mathbb{Q}$ 上超越的であることは自然対数の底 e や円周率 π のような超越数の存在から分かる (第 2 章参照).

α が F 上代数的ならば，それは F 上のある多項式を満たすので，F 上のある既約多項式を満たす．F は体であるから，$f \in F$ かつ $p(x) \in F[x]$ ならば，$f^{-1}p(x) \in F[x]$ でもある．これは，次のことを意味している．$p(x)$ の最高次の係数を a_n とするとき，$p(\alpha) = 0$ ならば $p_1(x) = a_n^{-1}p(x)$ は $F[x]$ のモニックな多項式であって，α は $p_1(x)$ を満たす．したがって，α が F 上代数的ならば，α が満たしているモニック既約多項式が存在する．次の結果はこの多項式は一意的に定まることを示している．

補題 6.1.3 $\alpha \in F'$ が F 上代数的ならば，$p(\alpha) = 0$ を満たすただ 1 つのモニック既約多項式 $p(x) \in F[x]$ が存在する．

このただ 1 つのモニック既約多項式を $irr(\alpha, F)$ で表す．

（**証明**）$f(\alpha) = 0, 0 \neq f(x) \in F[x]$ と仮定する．$f(x)$ を既約多項式に分解する．体には 0 でない零因子は存在しないので，これらの因子の 1 つ，$p_1(x)$ は

α を根としてもつ．$p_1(x)$ の最高次の係数を a_n とすれば，$a_n^{-1}p_1(x)$ は $F[x]$ のモニック既約多項式で α を根としてもつ．

以上によって，α を根としてもつモニック既約多項式が存在する．$p(x)$ をこのような多項式の中で次数最小のものとする．$p(x)$ がただ 1 つであることを示せばよい．

$g(x)$ を $g(\alpha) = 0$ を満たすもう 1 つのモニック既約多項式とする．$p(x)$ は最小次数であるから，$\deg p(x) \leq \deg g(x)$. 除法の定理によって，$q(x), r(x) \in F[x]$ が存在して

$$g(x) = q(x)p(x) + r(x). \tag{6.1.2}$$

ここで，$r(x) \equiv 0$ かまたは $\deg r(x) < \deg p(x)$.

α を (6.1.2) に代入して，次の式を得る．

$$g(\alpha) = q(\alpha)p(\alpha) + r(\alpha).$$

$g(\alpha) = p(\alpha) = 0$ であるから，この式は $r(\alpha) = 0$ を意味している．ところが $r(x)$ が多項式として 0 でないとすると，α は $r(x)$ の根となる．これは $p(x)$ の次数の最小性に矛盾する．したがって，$r(x) = 0$ であって，$g(x) = q(x)p(x)$ となる．$g(x)$ は既約であるから，多項式 $q(x)$ は定数（単元因子）でなければならない．しかし，このとき $g(x)$ と $p(x)$ は 2 つともモニックであるから，$q(x) = 1$ である．このことは，$g(x) = p(x)$ を意味しており，したがって $p(x)$ は一意的に定まる． ■

$\alpha \in F'$ が F 上代数的で，$p(x) = irr(\alpha, F)$ とする．そのとき，$\alpha \in E, F \subset E \subset F'$ を満たす最小の中間体 E が存在する．最小性とは，E' が $\alpha \in E'$ を満たすもう 1 つの中間体とすると，$E \subset E'$ となっている，ということを意味する．この最小の体の存在を確かめるために，$\alpha \in E'$ である F' の部分体 E' が存在することに注意しよう (すなわち，F' 自身がそうである). α を含んでいる F' のすべての部分体の共通集合を E とする．E は F' の部分体であり（演習問題参照），F' は α と F を含んでいる．さらに，この共通集合は α と F を含んでいる他のどの部分体にも含まれている．

この最小の部分体は非常に特別な形をしている．

定義 6.1.2 $\alpha \in F'$ が F 上代数的で，$p(x) = irr(\alpha, F) = a_0 + a_1x + \cdots +$

$a_{n-1}x^{n-1}+x^n$ とする．このとき，

$$F(\alpha)=\{f_0+f_1\alpha+\cdots+f_{n-1}\alpha^{n-1}\ ;\ f_i\in F\}$$

とおく．$F(\alpha)$ 上で成分ごとに加法と減法を定義し，乗法を等式

$$\alpha^n=-a_0-a_1\alpha-\cdots-a_{n-1}\alpha^{n-1}$$

を用いて，α^n 以上の α のベキを置き換えるという代数的手法によって定義する．

定理 6.1.2 $F(\alpha)$ は F の有限次拡大体で $[F(\alpha):F]=\deg irr(\alpha,F)=n$ を満たす．また，$F(\alpha)$ は F と α を含んでいる F' の最小の部分体である．

適当な α による $F(\alpha)$ の形の拡大を F の**単純拡大**という．

（証明） $F_{n-1}[x]$ はゼロ多項式と F 上 $n-1$ 次以下の全ての多項式の集合であった．この集合は F 上 n 次元のベクトル空間である．定義 6.1.2 において定義されたように，加法と減法に関しては $F_{n-1}[x]$ と同じであるから，$F(\alpha)$ は F 上 n 次元のベクトル空間である．ゆえに，それは可換群である．

乗法は多項式の乗法を経由して定義されているので，$F(\alpha)$ が単位元をもつ可換環であることを確かめるのは容易である．そこで，$F(\alpha)$ が体であることを示さなければならない．このために，$F(\alpha)$ の 0 でない元は乗法逆元をもつことを示す．

$0\neq g(x)\in F[x]$ とする．$\deg g(x)<n=\deg irr(\alpha,F)$ のとき，$g(\alpha)\neq 0$ である．何故ならば，$irr(\alpha,F)$ は α を根としてもつ最小次数の既約多項式であるから．

$h(x)\in F[x],\deg h(x)\geq n$ のとき，$h(\alpha)=h_1(\alpha)$ であるような多項式 $h_1(x)$ を見つけることができる．ここで $h_1(x)$ は

$$\alpha^n=-a_0-a_1\alpha-\cdots-a_{n-1}\alpha^{n-1}$$

を用いて α^n 以上の α のベキをより低い次数の和によって置き換えることによって得られる $n-1$ 次以下の多項式である．

次に，$g(\alpha)\in F(\alpha),g(\alpha)\neq 0$ と仮定する．対応している次数 $n-1$ 次以下の多項式 $g(x)\in F[x]$ を考える．$p(x)=irr(\alpha,F)$ は既約であるから，$g(x)$ と

$p(x)$ は互いに素，すなわち，$(g(x), p(x)) = 1$ である．ゆえに，ある多項式 $h(x), k(x) \in F[x]$ が存在して，次の式が成り立つ．

$$g(x)h(x) + p(x)k(x) = 1.$$

上の式に α を代入すると，次を得る．

$$g(\alpha)h(\alpha) + p(\alpha)k(\alpha) = 1.$$

しかし，$p(\alpha) = 0$ で，$h(\alpha) = h_1(\alpha) \in F(\alpha)$ であるから，

$$g(\alpha)h_1(\alpha) = 1.$$

したがって，$F(\alpha)$ において $h_1(\alpha)$ は $g(\alpha)$ の乗法逆元である．以上により，$F(\alpha)$ の 0 でない元はこのような逆元をもつので，$F(\alpha)$ は体となる．

定義によって，F は $F(\alpha)$ に含まれているので，$F(\alpha)$ は F の拡大体である．また $F(\alpha)$ の定義から，$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ が 1 つの基底であるから，$F(\alpha)$ の F 上の拡大次数は n である．したがって，$F(\alpha)$ は有限次拡大であり，ゆえに代数拡大となる．

$F \subset E \subset F'$ で $\alpha \in E$ とすると，E は体であるから，明らかに E は α のすべてのベキを含んでいる．ゆえに，E は $F(\alpha)$ を含む．したがって，$F(\alpha)$ は F と α を含んでいる最小の体となる． ■

例 6.1.3 $\mathbb{Q}$ 上の多項式 $p(x) = x^3 - 2$ を考える．これは $\mathbb{Q}$ 上既約であるが，根 $\alpha = 2^{1/3} \in \mathbb{R}$ をもつ．だから体 $\mathbb{Q}(\alpha) = \mathbb{Q}(2^{1/3})$ は $\mathbb{Q}$ と $2^{1/3}$ を含んでいる $\mathbb{R}$ の最小の部分体である．

ここで，$\mathbb{Q}(\alpha)$ は次のような集合である．

$$\mathbb{Q}(\alpha) = \{q_0 + q_1\alpha + q_2\alpha^2 \,;\, q_i \in \mathbb{Q}, \alpha^3 = 2\}.$$

はじめに，$\mathbb{Q}(\alpha)$ における加法と乗法の例を与える．

$g = 3 + 4\alpha + 5\alpha^2, h = 2 - \alpha + \alpha^2$ とする．このとき，

$$g + h = 5 + 3\alpha + 6\alpha^2$$

であり，また

$$\begin{aligned} gh &= 6 - 3\alpha + 3\alpha^2 + 8\alpha - 4\alpha^2 + 4\alpha^3 + 10\alpha^2 - 5\alpha^3 + 5\alpha^4 \\ &= 6 + 5\alpha + 9\alpha^2 - \alpha^3 + 5\alpha^4. \end{aligned}$$

ここで，$\alpha^3 = 2$ であるから，$\alpha^4 = 2\alpha$. したがって，

$$gh = 6 + 5\alpha + 9\alpha^2 - 2 + 5(2\alpha) = 4 + 15\alpha + 9\alpha^2.$$

次に，$\mathbb{Q}(\alpha)$ において，h の逆元の求め方を示そう．$h(x) = 2 - x + x^2, p(x) = x^3 - 2$ とする．第 3 章においてそうしたように，ユークリッドの互除法を用いて 1 を $h(x)$ と $p(x)$ の 1 次結合として表すと，

$$\begin{aligned} x^3 - 2 &= (x^2 - x + 2)(x + 1) + (-x - 4), \\ x^2 - x + 2 &= (-x - 4)(-x + 5) + 22. \end{aligned}$$

これより，

$$22 = (x^2 - x + 2)\{1 + (x + 1)(-x + 5)\} - \{(x^3 - 2)(-x + 5)\}.$$

すなわち，

$$1 = \frac{1}{22}\{(x^2 - x + 2)(-x^2 + 4x + 6)\} - \{(x^3 - 2)(-x + 5)\}.$$

α を代入して，$\alpha^3 = 2$ を用いると

$$1 = \frac{1}{22}\{(\alpha^2 - \alpha + 2)(-\alpha^2 + 4\alpha + 6)\}.$$

ゆえに，

$$h^{-1} = \frac{1}{22}(-\alpha^2 + 4\alpha + 6).$$

□

今，$\alpha, \beta \in F'$ を 2 つとも F 上代数的であるとして，$irr(\alpha, F) = irr(\beta, F)$ であると仮定する．$F(\alpha)$ の作り方から，$F(\alpha)$ は本質的に $F(\beta)$ と同じものであると見ることができる．この考えを正確に表現しよう．

定義 6.1.3 F', F'' を F の拡大体とする．**F-同型写像**とは，$\sigma : F' \to F''$ なる同型写像で F の任意の元 f に対して $\sigma(f) = f$ を満たすものである．すな

わち，F-同型写像とは，拡大体の同型写像であって，基礎体 F の各元を**固定**するものである．F', F'' が F-同型写像であるとき，この関係を $F' \underset{F}{\cong} F''$ によって表し，F' は F'' に同型である，という．

補題 6.1.4 $\alpha, \beta \in F'$ を F 上代数的な元とし，$irr(\alpha, F) = irr(\beta, F)$ と仮定する．このとき，$F(\alpha)$ は $F(\beta)$ に F-同型である．

(証明) $\sigma(\alpha) = \beta, \sigma(f) = f$ (すべての $f \in F$ に対して) によって，写像 $\sigma : F(\alpha) \to F(\beta)$ を定義する．この定義は σ が準同型写像であることを意味している．すなわち，σ は加法と乗法を保存する．σ は $F(\alpha)$ の元 $f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1}$ を $F(\beta)$ の元 $f_0 + f_1\beta + \cdots + f_{n-1}\beta^{n-1}$ に移す．このことより，σ が F-同型写像であることはすぐにわかる． ■

$\alpha, \beta \in F'$ が F 上代数的な 2 つの元とし，$(F(\alpha))(\beta)$ を $F(\alpha, \beta)$ により表す．このとき，$F(\alpha, \beta) = F(\beta, \alpha)$ が成り立つ．さて，基礎体上代数的な元の集合は代数的操作で閉じていることを示そう．このことより，代数的な元の集合は部分体をつくることがわかる．

補題 6.1.5 $\alpha, \beta \in F'$ を F 上代数的な元とすると，$\alpha \pm \beta, \alpha\beta, \alpha/\beta$ も F 上代数的である．

(証明) $\alpha, \beta \in F'$ は F 上代数的な元であるから，部分体 $F(\alpha, \beta)$ は F 上有限の拡大次数をもつ．ゆえに，それは F 上代数的である．今，$\alpha, \beta \in F(\alpha, \beta)$ であって，$F(\alpha, \beta)$ は部分体であるから，$\alpha \pm \beta, \alpha\beta, \alpha/\beta$ も $F(\alpha, \beta)$ の元である．$F(\alpha, \beta)$ は F の代数拡大であるから，これらの各元は F 上代数的である． ■

定理 6.1.3 F' を F の拡大体とすれば，F 上代数的な F' の元の集合は F' の部分体をなす．この部分体を F' における F の**代数的閉包**という．

(証明) $A_F(F')$ を F' の元で F 上代数的な元の集合とする．これは F を含んでいるから，$A_F(F') \neq \emptyset$. 前の補題より，それは加法，減法，乗法，除法に関して閉じている．したがって，$A_F(F')$ は体をつくる． ■

この節を次の最後の結果で締めくくろう．すなわち，すべての有限次拡大は有限回の単純拡大を続けることによって得られる．

定理 6.1.4　F' を F の有限次拡大体とすれば，有限個の代数的な元の集合 $\{\alpha_1, \ldots, \alpha_n\}$ が存在して，$F' = F(\alpha_1, \ldots, \alpha_n)$ と表される．

（**証明**）$[F' : F] = k < \infty$ と仮定する．そのとき，F' は F 上代数的である．$\alpha_1 \in F', \alpha_1 \notin F$ なる元を選ぶ．すると，$F \subset F(\alpha_1) \subset F'$ かつ $[F' : F(\alpha_1)] < k$. この拡大次数が 1 ならば，$F' = F(\alpha_1)$ となり証明は終わる．そうでないときは，$\alpha_2 \in F', \alpha_2 \notin F(\alpha_1)$ なる元を選ぶ．すると上のようにして，$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset F'$ であり，$[F' : F(\alpha_1, \alpha_2)] < [F' : F(\alpha_1)]$. 前と同様にして，この拡大次数が 1 ならば証明は終わる．そうでなければ，この操作を続ける．k は有限であるから，この操作は有限回で終わる．■

6.2　体への根の添加

前の節において，はじめに体 F の拡大体の存在を仮定しておいて，その拡大体の中で代数的な元を考察した．クロネッカーによる次の定理は基本的である．それは，任意に与えられた既約多項式 $f(x) \in F[x]$ に対して，$f(x)$ がその中に根をもつ F の拡大体 F' を構成できることを示しているからである．

定理 6.2.1（クロネッカーの定理）F を体として，$f(x)$ を F 上の既約多項式とする．そのとき，$f(x)$ がその中に根をもつ F の拡大体 F' が存在する．

定理 6.2.1 における $f(x)$ の根を含む拡大体の構成は一般的な代数的アプローチにより達成される．ここではその概略を述べる．はじめに，いくつかの準備をした後で定理 6.2.1 の証明をする．

定義 6.2.1　R を可換環[3] とする．部分環 $I \subset R$ は任意の $r \in R$ に対して $rI \subset I$ を満たすとき，**イデアル**であるという．

例 6.2.1　整数環 $\mathbb{Z}$ において，n の倍数全体の集合を $n\mathbb{Z} = \{nz\ ;\ z \in \mathbb{Z}\}$ とおく．このとき，$n\mathbb{Z}$ は部分環であって，$m \in \mathbb{Z}$ に対して $m(nz) = n(mz) \in n\mathbb{Z}$ が成り立つので $n\mathbb{Z}$ は $\mathbb{Z}$ のイデアルである．□

---

[3] イデアルは非可換環に対しても定義されるが，本書では必要がない．

例 6.2.2 R を可換環として，$r \in R$ する．$(r) = \{r_1 r\,;\, r_1 \in R\}$ を R における r のすべての倍数全体とする．このとき，(r) は r によって生成された**単項イデアル**と呼ばれるイデアルをつくる（演習問題参照）．

この言葉によれば，$n\mathbb{Z}$ は $\mathbb{Z}$ における単項イデアル (n) である． □

例 6.2.3 R を可換環，$I \subset R$ をイデアル，$r \in R$ とする．次のような集合を考える．

$$(r, I) = \{r_1 r + i_1\,;\, r_1 \in R, i_1 \in I\}.$$

このとき，(r, I) は r と I によって生成された**イデアル**と呼ばれるイデアルをつくる（演習問題参照）． □

定義 6.2.2 $I \subset R$ をイデアルとする．R の任意の元 r に対して，$r + I$ の形の部分集合を R における I の**剰余類**という．イデアル I のすべての剰余類の集合を R/I によって表す．

補題 6.2.1 R におけるイデアル I の剰余類の集合 R/I は R を分割する．

（**証明**）$r_1 - r_2 \in I$ によって，R 上に関係 $r_1 \sim r_2$ を定義する．これは同値関係である．したがって，その同値類は R を分割する．$r \in R$ について，その同値類 $[r]$ はまさに $r + I$ である． ■

イデアル I による同値類の集合 R/I の上に演算を次のように定義する．

(1) $(r_1 + I) \pm (r_2 + I) = (r_1 \pm r_2) + I$.
(2) $(r_1 + I)(r_2 + I) = (r_1 r_2) + I$.

このとき，次の定理は容易に確かめられる．

定理 6.2.2 与えられた可換環 R とイデアル I に対して，剰余類の集合 R/I は上で定義した演算に関して可換環をつくる．集合 $0 + I$ が R/I のゼロ元で，R が乗法単位元 1 をもてば集合 $1 + I$ が R/I の乗法単位元である．環 R/I はイデアル I を法とする**剰余環**と呼ばれる．

例 6.2.4 整数環 $\mathbb{Z}$ とイデアル $n\mathbb{Z}$ を考える．$\mathbb{Z}/n\mathbb{Z}$ を $n\mathbb{Z}$ による $\mathbb{Z}$ の剰余類の集合とする．

$x_1, x_2 \in \mathbb{Z}$ に対して，$x_1 - x_2 \in n\mathbb{Z}$(すなわち，$n|x_1 - x_2$) のとき，$x_1 \sim x_2$ と定義する．ゆえに n で割ったとき，異なった余りに対して異なっただけ剰余類がある．したがって，各 $x \in \mathbb{Z}, 0 \leq x \leq n-1$ に対してただ 1 つの剰余類が存在する．剰余類の加法と乗法は n を法とする加法と乗法によって定義される．以上より，$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. ここで，$\mathbb{Z}_n$ は n を法とする整数の全体である．□

定義 6.2.3 イデアル $I \subset R$ は $I \neq R$ であって，かつ任意の $r \in R, r \notin I$ に対して $(r, I) = R$ を満たすとき，**極大イデアル**であるという．

補題 6.2.2 R を単位元をもつ可換環とする．このとき，R/I が体であるための必要十分条件は I が極大イデアルとなることである．

（**証明**）I が極大イデアルであると仮定する．R/I が体であることを示す．R/I は単位元をもつ可換環であるから，ゼロでない元が乗法逆元をもつことを示せばよい．

$r \in R$ に対して，$\bar{r} = r + I$ をその対応している剰余類とする．$\bar{r} \in R/I, \bar{r} \neq \bar{0}$ と仮定する．すると，$\bar{0} = I$ は R/I のゼロ元であるから，$r \notin I$ である．I は極大イデアルであるから，$(r, I) = R$. ゆえに，$1 \in (r, I)$. したがって，$r_1 \in R, i_1 \in I$ が存在して，$r_1 r + i_1 = 1$ が成り立つ．剰余類の言葉では，

$$r_1 r \in 1 + I \text{ すなわち}, R/I \text{ において } \overline{r_1 r} = \bar{1}.$$

したがって，$\bar{r}_1$ は $\bar{r}$ の乗法逆元であるから，R/I は体となる．

逆に，R/I が体であると仮定して，I が極大イデアルであることを示す．$r \in R, r \notin I$ と仮定する．$\bar{r} \neq \bar{0}$ であるから，ある元 $r_1 \in R$ が存在して $\overline{r r_1} = \bar{1}$ が成り立つ．これは $r_1 r \in 1 + I$, すなわち，$r_1 r + i_1 = 1$ であることを意味している．したがって，$1 \in (r, I)$ となる．(r, I) はイデアルだから，$s \in R$ ならば $s \cdot 1 \in (r, I)$ である．ゆえに，$R \subset (r, I)$ であることが示され，$(r, I) \subset R$ は明らかであるから，$(r, I) = R$ を得る．以上により，I は R の極大イデアルである．■

以上の準備のもとに定理 6.2.1 を証明しよう．

（**証明**）(定理 6.2.1) F を体とし，$f(x) \in F[x]$ が F 上の既約多項式であると仮定しよう．$F[x]$ は単位元をもつ可換環である．$f(x)$ によって生成された $F[x]$ の単項イデアル $(f(x))$ を考える．

$g(x) \notin (f(x))$ と仮定すると，$g(x)$ は $f(x)$ の倍数ではない．$f(x)$ は既約であるから，$(f(x), g(x)) = 1$. したがって，ある多項式 $h(x), k(x) \in F[x]$ が存在して次の式が成り立つ．

$$h(x)f(x) + k(x)g(x) = 1.$$

左辺の元はイデアル $(g(x), f(x))$ に属しているので，単位元 1 もこのイデアルに属する．ゆえに，全体の環 $F[x]$ がこのイデアルに含まれる．$g(x)$ は任意であったから，これは単項イデアル環 $(f(x))$ が極大であることを示している．

$F' = F[x]/(f(x))$ とおく．補題 6.2.2 より，F' は体である．$F \subset F[x]$ であるから，$F \subset F'$ となることがわかる．$\bar{x}$ を x の剰余類とする．このとき，F' において $f(\bar{x}) = \overline{f(x)} = \bar{0}$. ゆえに，$\bar{x}$ は F' における $f(x)$ の根である．ここで，$\overline{f(x)}$ において $f(x)$ の上にある線は剰余類を表す．以上によって，既約多項式 $f(x)$ がその中に根をもつような体 F' を構成したことになる． ■

上記証明において x の $F' = F[x]/(f(x)$ における像を α とおく．そのとき，$F[x]$ に属する任意の多項式 $g(x)$ の像は $g(\alpha)$ となるので，F' は体であるが次のように書くことができる．

$$\begin{aligned} F'(x) = F[x]/(f(x)) &= \{g(\alpha)\ ;\ g(x) \in F[x]\} \\ &= \{a_0 + a_1\alpha + \cdots + a_n\alpha^n\ ;\ a_0, a_1, \cdots, a_n \in F\} \end{aligned}$$

ここでの α はあくまで $F' = F[x]/(f(x))$ における x の像 $\bar{x}$ として定義されたものである．前節では基礎体 F の拡大体 F' の元 α が代数的であるとすると，既約多項式 $irr(\alpha, F) = p(x)$ が定まり，F' の部分集合

$$\{f_0 + f_1\alpha + \cdots + f_n\alpha^n\ ;\ f_0, f_1, \cdots, f_n \in F\}$$

が F' の部分体 $F(\alpha)$ になることを示したのである．前節では，α が先にある拡大体 F' の中に存在していたのであり，この節では F と $F[x]$ と $f(x)$ が先にあって，それらから $f(x)$ の根 α を含む体 F' が構成されたのである．

例 6.2.5　x の $\mathbb{R}[x]/(x^2+1)$ における像を α とする．このとき，$\alpha^2+1=0$，すなわち，$\alpha^2=-1$ が成り立つ．すると，$\mathbb{R}$ の拡大体 $\mathbb{R}(\alpha)$ は

$$\mathbb{R}(\alpha)=\{a+b\alpha i\ ;\ a,b\in\mathbb{R},\alpha^2=-1\}$$

と表される．この体は複素数体 $\mathbb{C}$ に $\mathbb{R}$-同型である．

$$\mathbb{R}(\alpha)\simeq\mathbb{R}(i)\simeq\mathbb{C}. \qquad \square$$

6.3　最小分解体

これまで，与えられた体 F 上の既約多項式に対して，この既約多項式が根をもつ拡大体が存在することを見てきた．これを押し進めて，与えられた多項式がすべての根をもつような拡大体を求めてみよう．

定義 6.3.1　$0\neq f(x)\in F[x]$ で，F' が F の拡大体とする．$f(x)$ が F' において (F' は F であってもよい), 1 次因数に分解するとき，$f(x)$ は F' において**1 次因数に分解**するという．

F' は $f(x)$ が 1 次因数に分解する最小の拡大体であるとき，F 上 $f(x)$ の**最小分解体**という ($f(x)$ の最小分解体はその中で $f(x)$ がすべての可能な根をもつ最小の拡大体のことである).

F' が F 上の有限個の多項式に対して最小分解体であるとき，F' をその多項式の集合の**最小分解体**という．

定理 6.3.1　$0\neq f(x)\in F[x]$ とすると，F 上 $f(x)$ の最小分解体が存在する．

（**証明**）最小分解体は繰り返し根を添加することによって得られる．一般性を失わずして，$f(x)$ が F 上次数 n の既約多項式と仮定してよい．定理 6.2.1 より，$f(\alpha)=0$ を満たす α を含んでいる体 F' が存在する．このとき，$f(x)=(x-\alpha)g(x)\in F'[x], \deg g(x)=n-1$ と表される．帰納法の仮定より，$g(x)$ は最小分解体をもつので，$f(x)$ もそうである．■

次の章で最小分解体をさらに特徴づける．ここでは，6.1 節で導入したいくつかのアイデアにもどる．

F' が F の拡大体であるとき，F 上代数的な F' の元の集合は F' において F の代数的閉包と呼ばれる部分体をつくることを前に述べた（定理 6.1.3）．より一般的に，$F'[x]$ の定数でない任意の多項式が F' に根をもつとき，F' を**代数的閉体**という．

この述語によって代数学の基本定理を表現すると，複素数体は代数的閉体であるということになる．

次の結果は代数的閉体であることと，明らかに同値であるいくつかの条件を定式化している．

定理 6.3.2 F を体とするとき，次の各命題は同値である．

(1) F は代数的閉体である．

(2) すべての定数でない多項式 $f(x) \in F[x]$ は $F[x]$ で 1 次因数に分解する．

(3) F は真の代数拡大をもたない．すなわち，$F \subset E, F \neq E$ を満たす代数拡大 E は存在しない．

定義 6.3.2 F' が F の拡大体であるとする．F' が F 上代数的で，かつ F' は代数的閉体であるとき，F' を F の**代数的閉包**という．

例 6.3.1 この例においては代数学の基本定理，すなわち，$\mathbb{C}$ は代数的閉体であることを仮定する．$\mathbb{C}$ は $\mathbb{Q}$ 上代数的でないので，$\mathbb{C}$ は $\mathbb{Q}$ の代数的閉包でないことに注意しよう．しかしながら，代数的数 $A_{\mathbb{C}}$，すなわち，$\mathbb{Q}$ 上代数的な複素数の集合は $\mathbb{Q}$ の代数的閉包である．

これを見るために，まず，$A_{\mathbb{C}}$ は定義によって $\mathbb{Q}$ 上代数的である．そこで，$A_{\mathbb{C}}$ が代数的閉体であることを示す．$f(x) \in A_{\mathbb{C}}[x]$ とする．α が $f(x)$ の根ならば，$\alpha \in \mathbb{C}$ である．$A_{\mathbb{C}}$ は $\mathbb{Q}$ の代数拡大であり，α は $A_{\mathbb{C}}$ 上代数的だから，α は $\mathbb{Q}$ 上代数的である．したがって，$\alpha \in A_{\mathbb{C}}$ となるので $A_{\mathbb{C}}$ は代数的閉体である．

より一般的に，K が F の拡大体であって，K が代数的閉体であるとき，F の K における代数的閉包は F の代数的閉体である． □

1 つの多項式 $f(x) \in F[x]$ が与えられたとき，その最小分解体をつくることができた．証明が選択公理に基づいている次の結果は，上の手続きを拡張して任意の体の代数的閉包を得ることができることを示している．

定理 6.3.3 すべての体 F は代数的閉包をもち，F の任意の 2 つの代数的閉包は同型である．

6.4　置換と対称式

代数学の基本定理の第 3 番目の証明を得るために対称多項式の概念が必要である．この概念を導入するために，はじめに初等的な群論の基本的な考えのいくつかを振り返ってみよう．

定義 6.4.1 **群** G とは，次の条件を満たしている 1 つの 2 項演算をもつ集合のことである．演算は乗法によって表す．

(1) 演算は結合的である．すなわち，G のすべての元 $g_1, g_2, g_3 \in G$ に対して $(g_1g_2)g_3 = g_1(g_2g_3)$ が成り立つ．
(2) この演算に関する単位元が G に存在する．すなわち，G の任意の元 g に対して $1g = g1 = g$ を満たす元 1 が G に存在する．
(3) 任意の元 $g \in G$ はこの演算に関する逆元をもつ．すなわち，任意の元 $g \in G$ に対して $gg^{-1} = g^{-1}g = 1$ を満たす元 g^{-1} が G に存在する．

演算が可換ならば (すなわち，任意の $g_1, g_2 \in G$ に対して $g_1g_2 = g_2g_1$), 群 G は**アーベル群**と呼ばれる．群 G の要素の個数を G の**位数**といい，$|G|$ で表す．$|G| < \infty$ ならば，群 G は**有限群**である．群 G の部分集合 H は G と同じ演算に関して群になるとき，**部分群**という．$H \neq \emptyset$ であって，H はその演算と逆元をとる操作において，閉じているとき H は G の部分群であると言ってもよい．

群はある集合からそれ自身の上への可逆な写像からしばしば発生する．このような写像を**置換**という．

定義 6.4.2 T を集合としたとき，T から T の上への 1 対 1 写像を**置換**という．T 上のすべての置換の集合を S_T によって表す．

定理 6.4.1 任意の集合 T に対して，S_T は写像の合成に関して群をつくる．この群 S_T を T についての**対称群**という．T と T_1 が同じ濃度をもてば S_T

と S_{T_1} は同型[4]，すなわち $S_T \cong S_{T_1}$ が成り立つ．T が $|T| = n$ なる有限集合ならば，S_T は有限群でその位数は $|S_T| = n!$ である．

(証明) T のすべての置換の集合 S_T に対して，写像の合成が結合的であり，単位元をもち，逆元をもつ演算であることを示さねばならない．

$f, g \in S_T$ とする．このとき，f, g は T からそれ自身の上への 1 対 1 の写像である．合成写像 $f \circ g$ を考えよう．$f \circ g(t_1) = f \circ g(t_2)$ とすると，$f(g(t_1)) = f(g(t_2))$. f は 1 対 1 であるから，$g(t_1) = g(t_2)$ である．さらに，g もまた 1 対 1 であるから，$t_1 = t_2$ を得る．したがって，$f \circ g$ は 1 対 1 写像である．

$t \in T$ とする．f は上への写像であるから，ある元 $t_1 \in T$ が存在して $f(t_1) = t$ を満たす．さらに，g もまた上への写像であるから，ある元 $t_2 \in T$ が存在して $g(t_2) = t_1$ を満たす．これらを一緒にすると，$f(g(t_2)) = t$ が得られる．したがって，$f \circ g$ は上への写像である．以上によって，$f \circ g$ もまた T の置換であるから，写像の合成によって S_T 上に妥当な 2 項演算が定義される．

恒等写像 $1(t) = t$(任意の $t \in T$ に対して) は S_T 上の単位元であり，各置換の逆写像はその置換の逆元である．置換は上への 1 対 1 写像であるから，各置換に対してただ 1 つの逆写像が存在する．

最後に写像の合成は常に結合的であり，したがって，S_T は群をつくる．

T, T_1 が同じ濃度をもつとすると，上への 1 対 1 写像 $\sigma : T \to T_1$ が存在する．写像 $F : S_T \to S_{T_1}$ を次のように定義する．$f \in S_T$ に対して，$F(f)(t_1) = \sigma(f(\sigma^{-1}(t_1)))$ とする．$F(f)$ が同型写像であることを確かめるのは容易である．

最後に，$|T| = n < \infty$ と仮定して，$T = \{t_1, \ldots, t_n\}$ とおく．各 $f \in S_T$ は次のように表現される．

$$f = \begin{pmatrix} t_1 & \cdots & t_n \\ f(t_1) & \cdots & f(t_n) \end{pmatrix}.$$

各 t_1 に対して，$f(t_1)$ は n 個の選び方がある．f は 1 対 1 であるから，t_2 に対して，$f(t_2)$ は $n-1$ 個の選び方がある．これを続ければ t_n に対して，

[4]群の同型の定義は p.124 参照.

$f(t_n)$ はただ 1 つの選び方であるところに行きつく．積の法則により，f に対する選び方の数，すなわち S_T の位数は次のようである．

$$n(n-1)\cdots 1 = n!.$$

n 個の元をもつ集合に対して，S_T を S_n によって表す．これを n 個の文字についての**対称群**という．■

例 6.4.1　S_3 の 6 個の元を書き表し，その群の乗積表を与える．

3 つの元に $\{1,2,3\}$ と名前をつける．そのとき，S_3 の 6 個の元は次のようである．

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

S_3 に対する乗積表は，必要な合成を行うことによって直接に書き表すことができる．たとえば，

$$ac = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = d.$$

この合成は次のように考えられる．$a : 1 \to 2, 2 \to 3, 3 \to 1; c : 1 \to 2, 2 \to 1, 3 \to 3$ であるから，$ac : 1 \to 3, 2 \to 2, 3 \to 1$ となる．

少し観察をすれば，乗積表をつくるのは多少簡単になる．はじめに，$a^2 = b, a^3 = 1$. 次に，$c^2 = 1, d = ac, e = a^2c$. そして最後に $ac = ca^2$ を得る．

これらの関係から，次の乗積表が完成される．

	1	a	a^2	c	ac	a^2c
1	1	a	a^2	c	ac	a^2c
a	a	a^2	1	ac	a^2c	c
a^2	a^2	1	a	a^2c	c	ac
c	c	a^2c	ac	1	a^2	a
ac	ac	c	a^2c	a	1	a^2
a^2c	a^2c	ac	c	a^2	a	1

この表は，たとえば $(ac)a^2 = a(ca^2) = a(ac) = a^2c$ などと計算して作られた．さらに，S_3 は

$$S_3 =< a, c\,; a^3 = c^2 = 1, ac = ca^2 >$$

によって**表現**されると言うことができる．

このことは，S_3 は 3 つの**関係** $a^3 = 1, c^2 = 1, ac = ca^2$ をもつ 2 つの元 a, c によって**生成される**，あるいは，2 つの**生成元** a, c をもつ，と言い表せる．□

体の拡大における我々の研究の中で，その定式化を後で考察することになる重要な成果は次のようである．

補題 6.4.1　T を集合とし，T_1 をその部分集合とする．H を T_1 の**各元を固定**する S_T の部分集合とする．すなわち，$H = \{f \in S_T$; 任意の $t \in T_1$ に対して $f(t) = t\}$. このとき，H は S_T の部分群である．

（証明） $1 \in H$ であるから，$H \neq \emptyset$ である．$h_1, h_2 \in H$ と仮定する．$t_1 \in T_1$ として，$h_1 \circ h_2(t_1) = h_1(h_2(t_1))$ を考える．$h_2 \in H$ であるから，$h_2(t_1) = t_1$，また $h_1 \in H$ であるから，$h_1(t_1) = t_1$. したがって，$h_1 \circ h_2 \in H$ となる．ゆえに，H は合成に関して閉じている．h_1 が t_1 を固定すれば，h_1^{-1} も t_1 を固定するので，H は逆元をとる操作に関して閉じている．よって，H は部分群である．■

置換についてのこれらの考えを，体上のある多項式に適用する．

定義 6.4.3　$y_1, \ldots, y_n$ を体 F 上の不定元とする．多項式 $f(y_1, \ldots, y_n) \in F[y_1, \ldots, y_n]$ は $y_1, \ldots, y_n$ の任意の置換 σ によって不変であるとき，すなわち，$f(y_1, \ldots, y_n) = f(\sigma(y_1), \ldots, \sigma(y_n))$ であるとき，$y_1, \ldots, y_n$ の**対称式**という．

$F \subset F'$ を体の拡大で，$\alpha_1, \ldots, \alpha_n \in F'$ とする．F に係数をもつ式 $f(\alpha_1, \ldots, \alpha_n)$ は，$f(\alpha_1, \ldots, \alpha_n)$ が $\{\alpha_1, \ldots, \alpha_n\}$ の任意の置換 σ によって不変のとき，$\alpha_1, \ldots, \alpha_n$ に関して**対称**であるという．

例 6.4.2　F を体とし，$f_0, f_1 \in F$ とする．$h(y_1, y_2) = f_0(y_1 + y_2) + f_1(y_1 y_2)$ とおく．

$\{y_1, y_2\}$ について，2 つの置換がある．すなわち，$\sigma_1 : y_1 \to y_1, y_2 \to y_2$ と $\sigma_2 : y_1 \to y_2, y_2 \to y_1$ である．

これら 2 つの置換のうちのどちらの 1 つを $\{y_1, y_2\}$ に適用しても，$h(y_1, y_2)$ は不変である．したがって，$h(y_1, y_2)$ は対称式である．□

定義 6.4.4　$x, y_1, \ldots, y_n$ を体 F 上の不定元とする (または F 上の拡大体 F' の元とする). 次のような多項式を考える．

$$p(x, y_1, \ldots, y_n) = (x - y_1) \cdots (x - y_n).$$

$i = 1, \ldots, n$ に対して，$y_1, \cdots, y_n$ の i **次の基本対称式** s_i とは多項式 $p(x, y_1, \ldots, y_n)$ における x^{n-i} の係数を a_i とするとき，$(-1)^i a_i$ のことである．

例 6.4.3　y_1, y_2, y_3 を考える．このとき，

$$\begin{aligned} p(x, y_1, y_2, y_3) &= (x - y_1)(x - y_2)(x - y_3) \\ &= x^3 - (y_1 + y_2 + y_3)x^2 + (y_1 y_2 + y_1 y_3 + y_2 y_3)x - y_1 y_2 y_3. \end{aligned}$$

したがって，任意の体上の y_1, y_2, y_3 における 3 つの基本対称式は次のようである．

(1) $s_1 = y_1 + y_2 + y_3$.
(2) $s_2 = y_1 y_2 + y_1 y_3 + y_2 y_3$.
(3) $s_3 = y_1 y_2 y_3$.

一般に，上記の例のパターンは $y_1, \ldots, y_n$ に対して成り立つ．すなわち，

$$\begin{aligned} s_1 &= y_1 + y_2 + \cdots + y_n \\ s_2 &= y_1 y_2 + y_1 y_3 + \cdots + y_{n-1} y_n \\ s_3 &= y_1 y_2 y_3 + y_1 y_2 y_4 + \cdots + y_{n-2} y_{n-1} y_n \\ &\vdots \\ s_n &= y_1 \cdots y_n. \end{aligned}$$

□

基本対称式の重要性は，任意の対称式は基本対称式から組み立てられることにある．**対称式の基本定理**と呼ばれている次の定理の中でこれを明らかにしていこう．我々はこの重要な結果をたびたび利用することになる．また，この定理の完全な証明は第 6.7 節で与えられる．

定理 6.4.2（対称式の基本定理）P を体上の不定元に関する対称式とする，すなわち，$P \in F[y_1, \dots, y_n]$ で P が対称式であるならば，$P(y_1, \dots, y_n) = g(s_1, \dots, s_n)$ を満たす多項式 $g \in F[y_1, \dots, y_n]$ がただ 1 つ存在する．言い換えると，$y_1, \dots, y_n$ に関する任意の対称式は $y_1, \dots, y_n$ に関する基本対称式 $s_1, \dots, s_n$ の多項式として表される．

この定理より次の 2 つの補題が得られる．そして，これらは次の代数学の基本定理の証明において決定的な役割を果たす．

補題 6.4.2 $p(x) \in F[x]$ として，$p(x)$ は最小分解体 F' において，根 $\alpha_1, \dots, \alpha_n$ をもつと仮定する．このとき，$\alpha_1, \dots, \alpha_n$ に関する基本対称式は F に属する．

（証明） $p(x) = f_0 + f_1 x + \cdots + f_n x^n \in F[x]$ とする．$F'[x]$ において，$p(x)$ は 1 次因数に分解し，その根は $\alpha_1, \dots, \alpha_n$ である．ゆえに，$F'[x]$ において次のように表される．

$$p(x) = f_n(x - \alpha_1) \cdots (x - \alpha_n).$$

そのとき，この多項式の係数は $f_n(-1)^i s_i(\alpha_1, \dots, \alpha_n)$ である．ここで，$s_i(\alpha_1, \dots, \alpha_n)$ は $\alpha_1, \dots, \alpha_n$ に関する基本対称式である．しかしながら，$p(x) \in F[x]$ であるから，各係数は F に属する．したがって，各 i に対して $f_n(-1)^i s_i(\alpha_1, \dots, \alpha_n) \in F$ である．$f_n \in F$ であるから，$s_i(\alpha_1, \dots, \alpha_n) \in F$ である． ■

補題 6.4.3 $p(x) \in F[x]$ として，$p(x)$ は最小分解体に根 $\alpha_1, \dots, \alpha_n$ をもつと仮定する．さらに，$g(x) = g(x, \alpha_1, \dots, \alpha_n) \in F'[x]$ を仮定する．$g(x)$ が $\alpha_1, \dots, \alpha_n$ に関して対称式ならば $g(x) \in F[x]$ である．

（証明） $g(x) = g(x, \alpha_1, \dots, \alpha_n) \in F'[x]$ は $\alpha_1, \dots, \alpha_n$ に関して対称であるから，定理 6.4.2 より，それは $\alpha_1, \dots, \alpha_n$ の基本対称式によって表される対称式である．補題 6.4.2 より，これらは基礎体 F に属しており，したがって，$g(x)$ の係数は F に属する．以上によって，$g(x) \in F[x]$ を得る． ■

6.5　代数学の基本定理 ——証明 3

代数学の基本定理の第 3 の証明を述べる．

定理 6.5.1（代数学の基本定理）任意の複素係数の多項式は複素数の根をもつ．すなわち，複素数体は代数的閉体である．

その証明は以下の 4 つの補題にによってなされる．そのうちの 3 つは前に論じた．決定的なのは 4 番目のものである．これは任意の実数係数の多項式は複素数の根をもつ，というものである．

補題 6.5.1 任意の奇数次の実数係数の多項式は実数の根をもつ．

（**証明**）これは定理 3.4.1 であり，中間値の定理から得られる結果であった．(第 3.4 節参照). ■

補題 6.5.2 次数が 2 であるすべての複素多項式は複素数の根をもつ．

（**証明**）この命題は補題 3.4.1 である．2 次方程式の根の公式と任意の複素数は平方根をもつという事実から得られる．(第 3.4 節参照). ■

補題 6.5.3 定数でないすべての実多項式が複素数の根をもてば，定数でないすべての複素多項式は複素数の根をもつ．

（**証明**）この命題は定理 3.4.2 であり，複素多項式の共役の概念に基づいている (第 3.4 節参照). ■

さて，鍵となる補題を証明しよう．

補題 6.5.4 定数でないすべての実多項式は複素数の根をもつ．

（**証明**）$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x], n \geq 1, a_n \neq 0$ とする．

$n = 2^m q$（q は奇数) とおき，m についての帰納法を用いる．$m = 0$ ならば，$f(x)$ の次数は奇数であり，このとき，定理は補題 6.5.1 より正しい．そこで，定理は $d = 2^k q', (k < m, q'$ は奇数) を満たすすべての多項式に対して成り立つと仮定する．さて，$f(x)$ の次数を $n = 2^m q$ とする．

F' を $\mathbb{R}$ 上 $f(x)$ の最小分解体とし，その根を $\alpha_1, \cdots, \alpha_n$ とする．最小分解体の存在については第 6.3 節で論じた．これらの根の少なくとも 1 つは $\mathbb{C}$ に属していることを証明する (実際これらの根はすべて $\mathbb{C}$ に属しているが，補題を証明するためには少なくとも 1 つが $\mathbb{C}$ に属していることを示せばよい).

$h \in \mathbb{Z}$ として，次のような多項式を考える．

$$H(x) = \prod_{i<j}(x - (\alpha_i + \alpha_j + h\alpha_i\alpha_j)).$$

この多項式は $F'[x]$ に属している．$H(x)$ のつくりかたより，根の対 $\{\alpha_i, \alpha_j\}$ の個数は $n = 2^m q$ 個の元から 2 つの元を選ぶ選び方の個数に等しい．この数は次の式によって与えられる．

$$\frac{(2^m q)(2^m q - 1)}{2} = 2^{m-1}q(2^m q - 1) = 2^{m-1}q'.$$

ここで，q' は奇数である．したがって，$H(x)$ の次数は $2^{m-1}q'$ である．

$H(x)$ は根 $\alpha_1, \cdots, \alpha_n$ の対称式である．$\alpha_1, \cdots, \alpha_n$ は実多項式 $f(x)$ の根であるから，補題 6.4.3 より，最小分解体においてこれらの根に関する任意の対称式は実多項式でなければならない．

それゆえ，$H(x)$ は次数 $2^{m-1}q'$ をもち，$H(x) \in \mathbb{R}[x]$ である．帰納法の仮定によって，$H(x)$ は 1 つの複素根をもつ．このことは

$$\alpha_i + \alpha_j + h\alpha_i\alpha_j \in \mathbb{C}$$

を満たす対 $\{\alpha_i, \alpha_j\}$ が存在することを意味している．

h は任意の整数であったから，任意の整数 h_1 に対して

$$\alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}$$

を満たす根の対 $\{\alpha_i, \alpha_j\}$ が存在するということである．

h_1 を整数全体を動かす．このような根の対 $\{\alpha_i, \alpha_j\}$ は有限個であるから，少なくとも 2 つの異なる整数 h_1, h_2 が存在して次を満たす．

$$z_1 = \alpha_i + \alpha_j + h_1\alpha_i\alpha_j \in \mathbb{C}, \quad z_2 = \alpha_i + \alpha_j + h_2\alpha_i\alpha_j \in \mathbb{C}.$$

このとき，$z_1 - z_2 = (h_1 - h_2)\alpha_i\alpha_j \in \mathbb{C}$ であり，また $h_1, h_2 \in \mathbb{Z} \subset \mathbb{C}$ であるから，$\alpha_i\alpha_j \in \mathbb{C}$ となる．さらに，$h_1\alpha_i\alpha_j \in \mathbb{C}$. これより，$\alpha_i + \alpha_j \in \mathbb{C}$ である

ことがわかる．ゆえに，

$$p(x) = (x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j)x + \alpha_i \alpha_j \in \mathbb{C}[x].$$

$p(x)$ は次数 2 の複素多項式であるから，補題 6.5.2 よりその根は複素数である．したがって，$\alpha_i, \alpha_j \in \mathbb{C}$ が得られ，ゆえに $f(x)$ は複素数の根をもつ．

■

ここまで準備すれば，代数学の基本定理の証明を与えることは容易である．

（代数学の基本定理の証明） 補題 6.5.4 より，定数でないすべての実多項式は複素数の根をもつ．したがって，補題 6.5.3 より定数でないすべての実多項式が複素数の根をもてば，定数でないすべての複素多項式は複素数の根をもつことになる．これで基本定理が証明された．

6.6　応用——自然対数の底 e と 円周率 π の超越性

代数的数とは有理数体 $\mathbb{Q}$ 上代数的な複素数 $\alpha \in \mathbb{C}$ のことである．すなわち，ある 0 でない有理数係数の多項式 $p(x) \in \mathbb{Q}[x]$ が存在して，$p(\alpha) = 0$ を満足している複素数のことである．我々はこの章において，代数的数の集合 $\mathbf{A}$ は $\mathbb{C}$ の部分体をなすことを見た．**超越数**とは集合 $\mathbb{C} - \mathbf{A}$ の元のことである．第 2 章演習問題 2.7 で代数的数の集合 $\mathbf{A}$ は可算集合であり，したがって非可算個の超越数が存在することを証明した．しかし，これは純粋な存在証明であり，特別なある複素数が超越的であることを証明するのは非常に難しい．この節においては，代数学の基本定理とこの章において発展させた技術を用いて，自然科学において重要である定数，自然対数の底 e と円周率 π が超越的であることを証明する．

最初に少し準備が必要である．$\alpha \in \mathbb{C}$ が代数的であると仮定すると，ある 0 でない多項式 $f(x) \in \mathbb{Q}[x]$ が存在して，$p(\alpha) = 0$ を満たす．$\mathbb{Q}$ は体であるから，明らかに $f(x)$ はモニックなものをとることができる．したがって，α を根としてもつ次数が最小のモニックな既約多項式 $p_\alpha(x) \in \mathbb{Q}[x]$ が存在する．これを $\mathbb{Q}$ 上 α の**最小多項式**と呼ぶ．

整数係数の多項式 $f(x) = a_n x^n + \cdots + a_0, n \geq 1, a_n \neq 0, a_i \in \mathbb{Z}$ が $\gcd(a_1, \ldots, a_n) = 1$ を満たすとき，$f(x)$ を**原始多項式**という．α が代数的

数で $f(\alpha)=0, f(x)\in\mathbb{Q}[x]$ とすれば，はじめに $f(x)$ の係数に十分大きい整数をかけてすべて整数にした後，それらの係数の最大公約数で割れば $p(\alpha)=0, p(x)\in\mathbb{Z}[x]$ を満たす原始多項式 $p(x)$ が得られる．以上より，次の補題が得られた．

補題 6.6.1 複素数 α が代数的数であるための必要十分条件は原始多項式 $p(x)\in\mathbb{Z}[x]$ が存在して $p(\alpha)=0$ を満たすことである．

$p_\alpha(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0, n\geq 1, a_i\in\mathbb{Q}$ を $\mathbb{Q}$ 上 α の最小多項式とする．このとき，代数学の基本定理によって $p_\alpha(x)$ を $\mathbb{C}$ 上 において 1 次式に分解できる．

$$p_\alpha(x)=(x-\alpha_1)\cdots(x-\alpha_n),\ \alpha_i\in\mathbb{C}\ (i=1,\ldots,n).$$

ここで，ある $j\in\{1,\ldots,n\}$ に対して $\alpha=\alpha_j$ である．$p_\alpha(x)$ は $\mathbb{Q}$ 上既約であるから，$p_\alpha(x)=p_{\alpha_i}(x)\ (i=1,\ldots,n)$, かつ $\alpha_i\neq\alpha_j\ (i\neq j)$ である．もし，ある α_i が重複しており，$p_\alpha(x)$ の単根でなければ，α_i は形式的導関数 $p'_\alpha(x)$ の根でもある．ゆえに，$p_\alpha(x)$ と $p'_\alpha(x)$ の最大公約数 $d(x)$ の根である．$d(x)$ の次数は正であるが，$d(x)$ は $p'_\alpha(x)$ を割り切るので，$p_\alpha(x)$ の次数よりは小さい．これは矛盾である．

複素数 $\{\alpha_1,\ldots,\alpha_n\}$ は $\mathbb{Q}$ 上 α の**共役**と呼ばれている．

補題 6.6.2 $\alpha\in\mathbb{C}$ が代数的数ならば，その $\mathbb{Q}$ 上の共役 $\{\alpha_1,\ldots,\alpha_n\}$ は次の既約整多項式の根である．

$$q_\alpha(x)=b_nx^n+\cdots+b_1x+b_0\in\mathbb{Z}[x].$$

ここで，$n\geq 1, b_n>0,\ gcd(b_0,\ldots,b_n)=1$.

多項式 $q_\alpha(x)$ を $\mathbb{Q}$ 上 α の**最小整多項式**という．

ある $r\in\mathbb{Q}$ をとれば，$q_\alpha(x)=rp_\alpha(x)$ が成り立つことに注意しよう．

定義 6.6.1 複素数 $\alpha\in\mathbb{C}$ は，α を根としてもつあるモニックな整多項式が存在するとき**代数的整数**という．すなわち，$f(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_0, b_i\in\mathbb{Z}, n\geq 1$ なる多項式 $f(x)\in\mathbb{Z}[x]$ が存在して，$f(\alpha)=0$ を満たす．

補題 6.6.3 複素数 $\alpha \in \mathbb{C}$ が代数的整数ならば，そのすべての共役 $\alpha_1, \ldots, \alpha_n$ もまた代数的整数である．

（証明） $f(x) \in \mathbb{Z}[x]$ を $f(\alpha) = 0$ を満たすモニックな多項式とする．$i = 1, \ldots, n$ に対して $p_\alpha(x) = p_{\alpha_i}(x)$ であるから，$p_{\alpha_i}(x) \mid f(x)$ が成り立つ．ゆえに，$f(\alpha_i) = 0$ である．■

系 6.6.1 複素数 $\alpha \in \mathbb{C}$ が代数的整数ならば，その最小整多項式はモニックである．

（証明） $f(x) \in \mathbb{Z}[x]$ を $f(\alpha) = 0$ を満たすモニックな多項式とする．そのとき，すべての共役について，$f(\alpha_i) = 0$ が成り立つ．このとき，原始整多項式 $h(x) \in \mathbb{Z}[x]$ と $r \in \mathbb{Q}$ が存在して，$rq_\alpha(x)h(x) = f(x)$ を満たす．$q_\alpha(x)$ と $h(x)$ は原始的であり，$f(x)$ はモニックであるから $r = \pm 1$ である．ゆえに，$q_\alpha(x)$ はモニックである．■

複素数 $\alpha \in \mathbb{C}$ が代数的整数で，$\alpha_1, \ldots, \alpha_n$ をその共役とする．このとき，

$$(x - \alpha_1) \cdots (x - \alpha_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \in \mathbb{Z}[x].$$

ここで，$s_i = s_i(\alpha_1, \ldots, \alpha_n)$ は $\alpha_1, \ldots, \alpha_n$ の 第 n 次基本対称式である（前節参照）．したがって，この基本対称式は整数でなければならない．対称式についての基本定理から，代数的整数の共役に関する任意の対称式は整数であることがわかる．このことより，代数的整数を一般の代数的数の閉包的性質へ拡張する次の補題を得る．

補題 6.6.4 複素数 $\alpha, \beta \in \mathbb{C}$ が代数的整数ならば，$\alpha \pm \beta$, $\alpha\beta$ もまた代数的整数である．

（証明） $\alpha_1 = \alpha, \ldots, \alpha_n$ を α の共役とし，$\beta_1 = \beta, \ldots, \beta_m$ を β の共役とする．このとき，次の多項式を考える．

$$f(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)) = x^{n+m} + d_{n+m-1} x^{n+m-1} + \cdots + d_0.$$

係数 d_k は α_i, β_j に関する対称式である．上の注意より，$d_k \in \mathbb{Z}$ である（補題において用いた議論との類似性に注意せよ）．以上より，$\alpha_i + \beta_j$ は代数的整数である．$\alpha_i - \beta_j, \alpha_i\beta_j$ についても同様である．■

系 6.6.2 代数的整数の集合は $\mathbb{C}$ の部分環をつくる．さらに，代数的数のつくる体は代数的整数のつくる環の商体である．

定理 6.6.1 自然対数の底 e は超越数である．すなわち，e は $\mathbb{Q}$ 上超越的である．

（**証明**）$f(x) \in \mathbb{R}[x]$ を次数 $m \geq 1$ の多項式とする．$z_1 \in \mathbb{C}, z_1 \neq 0$ として，$\gamma : [0,1] \to \mathbb{C}, \gamma(t) = tz_1$ とおく．さらに，

$$I(z_1) = \int_\gamma e^{z_1 - z} f(z) dz = \left(\int_0^{z_1} \right)_\gamma e^{z_1 - z} f(z) dz$$

とする．$\left(\int_0^{z_1} \right)_\gamma$ によって，γ に沿って 0 から 1 へ向かう積分を表す．次の式が成り立つことを思い出そう．

$$\left(\int_0^{z_1} \right)_\gamma e^{z_1 - z} f(z) dz = -f(z_1) + e^{z_1} f(0) + \left(\int_0^{z_1} \right)_\gamma e^{z_1 - z} f'(z) dz.$$

繰り返しこの積分を行うことによって，次を得る．

(1) $I(z_1) = e^{z_1} \displaystyle\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z_1)$.

$|f|(z)$ を $f(z)$ の係数をそれらの絶対値で置き換えた多項式とする．$|e^{z_1 - z}| \leq e^{|z_1 - z|} \leq e^{|z_1|}$ であるから，次の式を得る．

(2) $|I(z_1)| \leq |z_1| e^{|z_1|} |f|(|z_1|)$.

さて，e が代数的数であると仮定する．すなわち，

(3) ある整数 $n \geq 1$ と整数 $q_0 \neq 0, q_1, \ldots, q_n \neq 0$ に対して，$q_0 + q_1 e + \cdots + q_n e^n = 0$ が成り立つ．ここで，$q_0, q_1, \ldots, q_n$ の最大公約数は 1 である．

p を十分大きな素数として，多項式 $f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p$ を考える．この多項式に関する $I(z_1)$ を考察する．

$$J = q_0 I(0) + q_1 I(1) + \cdots + q_n I(n)$$

とおく．(1) と (3) より，次の式を得る．

$$J = -\sum_{j=0}^{m} \sum_{k=0}^{n} q_k f^{(j)}(k).$$

ここで，$(q_0+q_1e+\cdots+q_ne^n)(\sum_{j=0}^m f^{(j)}(0))=0$ だから $m=(n+1)p-1$.

さて，$j<p, k>0$ に対して $f^{(j)}(k)=0$ であり，$j<p-1$ ならば $k\geq 0$ に対して，$f^{(j)}(k)=0$．したがって，$j=p-1, k=0$ 以外のすべて j,k に対して $f^{(j)}(k)$ は $p!$ によって割り切れる整数である．さらに，$f^{(p-1)}(0)=(p-1)!(-1)^{np}(n!)^p$ であり，ゆえに，$p>n$ ならば $f^{(p-1)}(0)$ は $(p-1)!$ によって割り切れるが，$p!$ では割り切れない整数である．

したがって，$p>|q_0|$ かつ $p>n$ ならば，J は $(p-1)!$ によって割り切れる 0 でない整数である．よって，$p>n, p>|q_0|$ とすれば $|J|\geq(p-1)!$.

さて，$|f|(k)\leq(2n)^m$ である．(2) とこの式より，p とは独立な数 c に対して次の式を得る．

$$|J|\leq|q_1|e|f|(1)+\cdots+|q_n|ne^n|f|(n)\leq c^p.$$

したがって，

$$(p-1)!\leq|J|\leq c^p.$$

すなわち，

$$1\leq\frac{|J|}{(p-1)!}\leq c\frac{c^{p-1}}{(p-1)!}.$$

$p\to\infty$ のとき，$\dfrac{c^{p-1}}{(p-1)!}\to 0$ であるから，これは矛盾である．以上により，e は超越的である． ■

次に円周率 π の超越性のほうに議論を移そう．このために，次の補題が必要である．

補題 6.6.5　$\alpha\in\mathbb{C}$ を代数的数と仮定し，多項式 $f(x)=a_nx^n+\cdots+a_0\in\mathbb{Z}[x], n\geq 1, a_n\neq 0$ は $f(\alpha)=0$ を満たしていると仮定する．このとき，$a_n\alpha$ は代数的整数である．

（証明）

$$\begin{aligned} a_n^{n-1}f(x) &= a_n^nx^n+a_n^{n-1}a_{n-1}x^{n-1}+\cdots+a_n^{n-1}a_0 \\ &= (a_nx)^n+a_{n-1}(a_nx)^{n-1}+\cdots+a_n^{n-1}a_0 \\ &= g(a_nx)=g(y)\in\mathbb{Z}[y]. \end{aligned}$$

ここで，$y = a_n x$ であり，$g(y)$ はモニックである．このとき，$g(a_n\alpha) = 0$. したがって，$a_n\alpha$ は代数的整数である． ■

定理 6.6.2 円周率 π は超越数である．すなわち，π は $\mathbb{Q}$ 上超越的である．

(証明) π は代数的数であると仮定する．このとき，$\theta = i\pi$ も代数的数である．$\theta_1 = \theta, \theta_2, \ldots, \theta_d$ を θ の共役とする．

$$p(x) = q_0 + q_1 x + \cdots + q_d x^d \in \mathbb{Z}[x],\ q_d > 0,\ gcd(q_0, \ldots, q_d) = 1$$

を $\mathbb{Q}$ 上 θ の最小整多項式とする．$\theta_1 = \theta, \theta_2, \ldots, \theta_d$ はこの多項式の根である．$t = q_d$ とおく．補題 6.6.5 より $t\theta_i$ はすべての i に対して代数的整数である．$e^{i\pi} + 1 = 0$ と $\theta_1 = i\pi$ より，次の式を得る．

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_d}) = 0.$$

左辺の積は 2^d 個の項 e^{ϕ} の和として表現できる．ここで，$\phi = \epsilon_1\theta_1 + \cdots + \epsilon_d\theta_d, \epsilon_i = 0$ または 1 である．n を $\epsilon_1\theta_1 + \cdots + \epsilon_d\theta_d$ が 0 でないような項の数とし，これらに $\alpha_1, \ldots, \alpha_n$ と名前をつける．すると，

(4) $q + e^{\alpha_1} + \cdots + e^{\alpha_n} = 0,\ q = 2^d - n > 0$

が成り立つ．ここで，すべての $t\alpha_i$ は代数的整数であることを思い出そう．そこで，十分大きな素数 p に対して次の多項式を考える．

$$f(x) = t^{np} x^{p-1} (x - \alpha_1)^p \cdots (x - \alpha_n)^p.$$

α_i は代数的数であり，$\alpha_1, \ldots, \alpha_n$ に関する基本対称式は有理数であるから，$f(x) \in \mathbb{R}[x]$ が成り立つ．

$I(z_1)$ を定理 6.6.1 の証明において定義されたものとし，

$$J = I(\alpha_1) + \cdots + I(\alpha_n)$$

とおく．定理 6.6.1 の証明における (1) と上の式 (4) より 次の式を得る．

$$J = -q \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} \sum_{k=1}^{n} f^{(j)}(\alpha_k).$$

ただし，$m = (n+1)p - 1$ である．

さて，$t\alpha_i$ は代数的整数であるから，$\sum_{k=1}^{n} f^{(j)}(\alpha_k)$ は $t\alpha_1, \ldots, t\alpha_n$ に関する整係数の対称式である．対称式に関する基本定理より，$\sum_{j=0}^{m}\sum_{k=1}^{n} f^{(j)}(\alpha_k)$ は整数である．さらに，$j < p$ に対して，$f^{(j)}(\alpha_k) = 0$ が成り立つ．ゆえに，$\sum_{j=0}^{m}\sum_{k=1}^{n} f^{(j)}(\alpha_k)$ は $(p-1)!$ によって割り切れる整数である．

$j \neq p-1$ ならば，$f^{(j)}(0)$ は $p!$ によって割り切れる整数である．$f^{(p-1)}(0) = (p-1)!(-t)^{np}(\alpha_1 \cdots \alpha_n)^p$ は $(p-1)!$ によって割り切れるが，p を十分大きくすれば $p!$ によって割り切れない．特に，これは $p > |t^n(\alpha_1 \cdots \alpha_n)|$ のとき正しく，また $p > q$ のときも正しい．

定理 6.6.1 の証明における (2) より，p に独立なある数 c に対して次を得る．

$$|J| \leq |\alpha_1|e^{|\alpha_1|}|f|(|\alpha_1|) + \cdots + |\alpha_n|e^{|\alpha_n|}|f|(|\alpha_n|) \leq c^p.$$

定理 6.6.1 の証明と同様にして，この式より次の式が得られる．

$$(p-1)! \leq |J| \leq c^p.$$

すなわち，

$$1 \leq \frac{|J|}{(p-1)!} \leq c\,\frac{c^{p-1}}{(p-1)!}.$$

前と同様に，$p \to \infty$ のとき，$\dfrac{c^{p-1}}{(p-1)!} \to 0$ であるから，これは矛盾である．以上によって，π は超越数であることが示された．■

6.7　対称式の基本定理

代数学の基本定理の第 3 の証明において，n 変数の不定元に関する任意の対称式はこれらの不定元に関する基本対称式の多項式であるという事実を用いた．そしてさらに，e と π の超越性の証明においても，対称式の基本定理と呼んでいる，この重要な定理を用いた．この節において，この定理の証明を与える．

R を整域とする．$x_1, \ldots, x_n$ を R 上の不定元とし，$R[x_1, \ldots, x_n]$ をこれらの不定元に関する多項式環とする．任意の多項式 $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ は $ax_1^{i_1} \cdots x_n^{i_n}$ $(a \in R)$ なる形の**単項式**の和として構成されている．

2 つの単項式 $ax_1^{i_1}\cdots x_n^{i_n}$ $(a\neq 0)$, $bx_1^{j_1}\cdots x_n^{j_n}$ $(b\neq 0)$ について，各指数の差

$$i_1-j_1, i_2-j_2, \ldots, i_n-j_n$$

のなかで，0 でない最初のものが正であるとき，単項式 $ax_1^{i_1}\cdots x_n^{i_n}$ $(a\neq 0)$ は単項式 $bx_1^{j_1}\cdots x_n^{j_n}$ $(b\neq 0)$ より**高い**という．多項式 $f(x_1,\ldots,x_n)$ の最も高い単項式を $HG(f)$ で表す．

補題 6.7.1 $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$ に対して，$HG(fg)=HG(f)HG(g)$ が成り立つ．

（**証明**）不定元の数 n についての帰納法を用いる．$n=1$ については明らかに成り立つので，$n\geq 2$ として，$k<n$ なる k 個の不定元のすべての多項式について，この補題が成り立つと仮定する．最初の不定元 x_1 の指数によって多項式を順序付けると，

$$\begin{aligned} f(x_1,\ldots,x_n) &= x_1^r\phi_r(x_2,\ldots,x_n)+x_1^{r-1}\phi_{r-1}(x_2,\ldots,x_n) \\ &\quad +\cdots+\phi_0(x_2,\ldots,x_n), \\ g(x_1,\ldots,x_n) &= x_1^s\psi_s(x_2,\ldots,x_n)+x_1^{s-1}\psi_{s-1}(x_2,\ldots,x_n) \\ &\quad +\cdots+\psi_0(x_2,\ldots,x_n). \end{aligned}$$

このとき，$HG(fg)=x_1^{r+s}HG(\phi_r\psi_s)$ が成り立つ．帰納法の仮定によって，$HG(\phi_r\psi_s)=HG(\phi_r)HG(\psi_s)$ が成り立つ．したがって，

$$HG(fg)=x_1^{r+s}HG(\phi_r)HG(\psi_s)=(x_1^rHG(\phi_r))(x_1^sHG(\psi_s))=HG(f)HG(g).$$

■

n 変数の不定元に関する基本対称式はつぎのようなものであった (第 6.4 節参照).

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n, \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ s_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n, \\ &\vdots \\ s_n &= x_1x_2\cdots x_n. \end{aligned}$$

これらの対称式は多項式 $p(x, x_1, \ldots, x_n) = (x - x_1)\cdots(x - x_n)$ をつくることによって得られる．$x_1, \ldots, x_n$ に関する第 i 次の基本対称式は $(-1)^i a_i$ である．ただし，a_i は $p(x, x_1, \ldots, x_n)$ における x^{n-i} の係数である．

一般に，$1 \leq k \leq n$ に対して

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

ただし，和は $i_1, \cdots, i_k$ $(i_1 < i_2 < \cdots < i_k)$ なる添数の 2 項係数 $\binom{n}{k}$ 個のすべての異なる組にわたって足すものとする．

さらに，多項式 $s(x_1, \ldots, x_n)$ は，$\{x_1, \ldots, x_n\}$ の任意の置換 σ によって不変のとき，すなわち，$s(x_1, \ldots, x_n) = s(\sigma(x_1), \ldots, \sigma(x_n))$ であるとき **対称式** と呼んだ (定義 6.4.3 参照)．

補題 6.7.2　対称式 $s(x_1, \ldots, x_n)$ の最も高い単項式 $ax_1^{k_1} \cdots x_n^{k_n}$ $(a \neq 0)$ においては，$k_1 \geq k_2 \geq \cdots \geq k_n$ が成り立つ．

（証明） ある $i < j$ に対して，$k_i < k_j$ であると仮定する．そのとき，対称式として，$s(x_1, \ldots, x_n)$ は単項式 $ax_1^{k_1} \cdots x_i^{k_j} \cdots x_n^{k_n}$ を含まなければならない．ところが，この単項式は $ax_1^{k_1} \cdots x_i^{k_i} \cdots x_n^{k_n}$ より高い．これは矛盾である． ■

補題 6.7.3　積 $s_1^{k_1-k_2} s_2^{k_2-k_3} \cdots s_{n-1}^{k_{n-1}-k_n}\ s_n^{k_n} (k_1 \geq k_2 \geq \cdots \geq k_n)$ は最も高い単項式 $x_1^{k_1} \cdots x_n^{k_n}$ をもつ．

（証明） 対称式の定義より，次が成り立つ．

$$HG(s_k^t) = (x_1x_2\cdots x_k)^t,\ 1 \leq k \leq n,\ t \geq 1.$$

補題 6.7.1 より,

$$HG(s_1^{k_1-k_2}s_2^{k_2-k_3}\cdots s_{n-1}^{k_{n-1}-k_n}s_n^{k_n}) = x_1^{k_1-k_2}(x_1x_2)^{k_2-k_3}\cdots(x_1\cdots x_{n-1})^{k_{n-1}-k_n}\cdots(x_1\cdots x_n)^{k_n} = x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.$$ ■

定理 6.7.1 $s(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$ を対称式とする．このとき，$s(x_1,\ldots,x_n)$ は R に係数をもつ基本対称式 $s_1,\ldots,s_n$ の多項式 $f(s_1,\ldots,s_n)$ として一意的に表される．

（**証明**）最も高い単項式の大きさに関する帰納法によって，多項式 f の存在を証明する．対称式の最も高い単項式において，すべての指数が 0 ならば，その多項式は定数である．すなわち，R の元であるから，このとき証明することは何もない．

今，$s(x_1,\cdots,x_n)$ の最高次の単項式より低い最高次の単項式をもつ任意の対称式は基本対称式に関する多項式として表すことができると仮定する．$ax_1^{k_1}\cdots x_n^{k_n}$, $a\neq 0$ を $s(x_1,\cdots,x_n)$ の 最高次の単項式とする．

$$t(x_1,\cdots,x_n) = s(x_1,\cdots,x_n) - as_1^{k_1-k_2}\cdots s_{n-1}^{k_{n-1}-k_n}s_n^{k_n}$$

とおく．明らかに，$t(x_1,\cdots,x_n)$ はもう 1 つの対称式である．補題 6.7.3 より，$t(x_1,\cdots,x_n)$ の 最高次の単項式は $s(x_1,\cdots,x_n)$ のそれよりも低い．したがって，$t(x_1,\cdots,x_n)$ は $s_1,\ldots,s_n$ に関する多項式として表されるので $s(x_1,\cdots,x_n)=t(x_1,\cdots,x_n)+as_1^{k_1-k_2}\cdots s_{n-1}^{k_{n-1}-k_n}s_n^{k_n}$ もそうである．

表現の一意性を示すために，$s(x_1,\cdots,x_n)=f(x_1,\cdots,x_n)=g(x_1,\cdots,x_n)$ と仮定する．そのとき，$f(x_1,\cdots,x_n)-g(x_1,\cdots,x_n)=h(x_1,\cdots,x_n)=\phi(x_1,\cdots,x_n)$ は $x_1,\ldots,x_n$ に関するゼロ多項式である．2 つの異なった $s_1,\cdots,s_n$ に関するベキの積は異なった最高次の単項式をもつので，$h(x_1,\cdots,x_n)$ を $x_1,\ldots,x_n$ のベキの積の和として表せば，すべての係数は消える．このことはこれまでの一連の補題からわかる．以上によって，f と g は同じであることが示され，定理が証明された． ■

演習問題

6.1　$p(x)=x^2+x+1$ とする．

(a) $p(x)$ は $\mathbb{Q}$ 上既約であることを示せ．

(b) α を $p(x)$ の根として，$g=2+\alpha, h=1-\alpha$ とおく．このとき，$g+h, gh$ と h^{-1} を求めよ．

(c) 体 $\mathbb{Q}(\alpha)$ において，1 次方程式 $2g+h=5$ を解け．

6.2　α, β は 2 つとも F 上既約でかつ，$irr(\alpha, F) = irr(\beta, F)$ と仮定する．補題 6.1.4 の証明において，与えられた写像は実際同型であることを確かめよ．

6.3　R を可換環とし，$r \in R$ とする．$(r) = \{r_1 r\,;\ r_1 \in R\}$ と表す．(r) がイデアルであることを確かめよ．

6.4　$I \neq R$ でかつ $r_1 r_2 \in I$ ならば $r_1 \in I$ かまたは $r_2 \in I$ を満たすとき，イデアル I を**素イデアル**という．このとき，次を示せ．

(a) $m\mathbb{Z}$ が素イデアルであるための必要十分条件は m が素数なることである．

(b) R を単位元をもつ可換環とする．I が素イデアルならば剰余環 R/I は整域である．

6.5　F を体とする．F のイデアルは全体 F か (0) であることを示せ．

6.6　$I \subset R$ はイデアルで，$r \in R, r \notin I$ とする．このとき，$(r, I) = \{r_1 r + i_1\,;\ r_1 \in R, i_1 \in I\}$ は I と異なるイデアルであることを示せ．

6.7　$F \subset E \subset F'$ とする．$\{\alpha_1, \ldots, \alpha_n\}$ を F 上 E の基底とし，$\{\beta_1, \ldots, \beta_m\}$ を E 上 F' の基底とするとき，mn 個の積 $\{\alpha_i \beta_j\}$ は F 上 F' の基底であることを証明せよ（ヒント：$\{\alpha_i \beta_j\}$ が F 上 F' の基底であることを証明するためには，(1) それらが F 上で F' を生成し，そして (2) それらが 1 次独立であることを示さねばならない．(1) を示すには，$g \in F'$ とする．$\{\beta_1, \ldots, \beta_m\}$ は E 上 F' の基底であるから，$g = e_1 g_1 + \cdots + e_m g_m$ $(e_i \in E)$ と表される．次に，各 e_i を $\{\alpha_1, \ldots, \alpha_n\}$ の 1 次結合で表し，上の式に代入すればよい．(2) を示すには，$f_1 \alpha_1 \beta_1 + \cdots + f_{mn} \alpha_n \beta_m$ $(f_i \in F)$ と仮定する．β_i に関する 1 次結合と考えて，$\{\beta_i\}$ の 1 次独立性を使う．次に，各係数において，$\{\alpha_i\}$ の 1 次独立性を使う）．

6.8　K を E の代数拡大とし，E を F の代数拡大とする．このとき，K は F の代数拡大であることを示せ．

6.9　F' を F の有限次拡大体とし，$\alpha \in F'$, $n = \deg irr(\alpha, F)$ とする．この

とき，n は $[F':F]$ の約数であることを示せ．

6.10 $F \subset D$ とする．ここで，F は体であり，D は F と同じ乗法単位元をもつ整域とする．このとき，D は F 上のベクトル空間である．D が F 上有限次元ならば，D は体となることを示せ．

6.11 最初の 5 つの基本対称式を書き表しなさい．

6.12 D_3 を正 3 角形のシンメトリーのつくる群とする．

(1) $|D_3| = 6$ であることを示せ．

(2) D_3 の成分を表示し，乗積表をつくりなさい．

(3) $S_3 \cong D_3$ を示せ．

6.13 D_4 を正方形のシンメトリーのつくる群とする．$|D_4| = 6$ であることを示し，D_4 の成分を表示し，乗積表をつくりなさい．さらに，$D_4 \ncong S_4$ を示せ．一般に，正 n 角形のシンメトリーのつくる群についてはどうであろうか？

第7章

ガロア理論

7.1　ガロア理論展望

前の章において，代数学の基本定理の代数的な証明を与えた．この証明は，任意の多項式に対する最小分解体が存在すること，奇数次の実数係数の多項式は実根をもつこと，複素数は常にその平方根をもつこと，すなわち，このことは任意の 2 次方程式は複素数体 $\mathbb{C}$ において可解であることを意味している，という一連の事実に基づいていた．この章においては，前の章の第 3 の証明によって暗示された証明，ガロア理論と呼ばれているより一般的なアイデアを巻き込んだ証明を与えよう．

ガロア理論は体の代数拡大の理論，方程式論と有限群論の相互関係を扱う数学の分野である．体の代数拡大についてのガロア理論の基礎の多くは前章において導入されている．

この理論は 1830 年頃エバリスト・ガロアによって，5 次方程式のベキ根による不可解性の研究のなかで導入された．その不可解性については，もう少し早くルフィニと，そして独立にアーベルによって証明されていたが，ガロアは最初に体の拡大と置換群の間に密接な関係のあることに気が付いた[5]．この研究をする中で，彼は有限群の研究を創始した．彼の定義は実際には置換の限られた集合に対するものであったけれども，抽象的な概念として群という言葉を最初に用いたのである．

[5]いくつかの文献によればルフィニの証明は完全なものではなかった．

ガロアが発展させた方法は 5 次および 5 次以上の方程式の不可解性の証明を容易にするだけではなく，我々を他の応用へと導き，さらにそれ自身大きな理論へと発展していった．しかしながらこの章においては，ガロア理論のなかの代数学の基本定理に関連のある部分のみを考察することにしよう．

ガロア理論の主要なアイデアは，**ガロア拡大**と呼ばれているある特別な代数拡大に対して**ガロア群**と呼ばれる群を結びつけることである．体の拡大の性質はより調べやすい群の性質に反映される．このようにして，たとえば，ベキ根による可解性は可解群という群の性質に翻訳される．5 次あるいはそれ以上の代数方程式に対して，そのガロア群が可解でないようなものが存在することを示すことにより，ベキ根による解の公式が作れないことが証明できることになる．

方程式論との結びつきは次のようである．$f(x)$ がある体 F 上の多項式による方程式とするとき，その最小分解体 K をつくることができる．これはガロア拡大であり，この拡大に対して，**方程式のガロア群**と呼ばれるガロア群がある．前と同様にして，この群の性質はこの方程式の性質を反映する．

ガロア理論は部分的に有限群の理論に依存している．したがって，次の節においてこの理論から基本的に必要である結果を考察する．

第 7.3 節において，ガロア拡大を定義している正規拡大と分離拡大の性質を導入し，続く節においてガロア群とその構造を調べる．次に，ガロア群とガロア拡大の間の相互関係を表しているガロア理論の基本定理の結果を要約する．第 7.6 節でこれら適切なすべての道具を用いて代数学の基本定理の第 4 番目の証明を与える．最後に，この章をガロア理論の 2 つの付加的な応用を与えて終えることにする．最初のものは，5 次方程式のベキ根による不可解性の証明のスケッチであり，第 2 のものは定規とコンパスによる幾何的な作図とそれらの代数的な解釈についての議論である．

我々の目的はガロア理論の主要な結果に急いで到達し，代数学の基本定理の第 4 番目の証明を与えることである．それで，途中にある多くのより難しい証明は省略される．

7.2　有限群からの準備

この節では有限群論からのいくつかの基本的な結果を見直す．群 G とは次の条件を満たしている 1 つの 2 項演算（これを乗法によって表す）をもつ集合のことである (第 6.4 節参照)．

(1) 与えられた演算は結合的である．
(2) この演算に関する単位元が存在する．
(3) この演算に関して，G の各元 g は逆元をもつ．

さらに，演算が可換であれば，群は**アーベル群**と呼ばれる．群 G の**位数**とは G の元の個数のことであり，$|G|$ で表す．$|G| < \infty$ ならば，G は**有限群**である．G の部分集合 H は $H \neq \emptyset$ でかつ G と同じ演算に関して群であるとき，G の**部分群**という．言い換えると，H は $H \neq \emptyset$ でかつ，H は演算と逆元をとる操作について閉じているとき，G の部分群である．

第 6.4 節で説明したように，群はしばしばある集合からそれ自身の上への可逆な写像から生じる．このような写像は**置換**と呼ばれた．n 個の要素をもつ集合上のすべての置換の集合つくる群は n 個の文字についての**対称群**と呼ばれ，S_n によって表わされた．

置換群の一種として，自己同型群が得られる．R と S が代数的構造（群，環，体，ベクトル空間等）をもつとする．このとき，写像 $f : R \to S$ はそれらの代数的演算を保存するとき**準同型写像**と呼ばれる．このことは，それぞれ次の式が成り立つことを意味している．

(1) R, S が群のとき，$f(r_1 r_2) = f(r_1)f(r_2)$.
(2) R, S が環または体のとき，$f(r_1 + r_2) = f(r_1) + f(r_2)$,　$f(r_1 r_2) = f(r_1)f(r_2)$.
(3) R, S がベクトル空間のとき，c をスカラーとして $f(r_1 + r_2) = f(r_1) + f(r_2)$,　$f(cr_1) = cf(r_1)$.

準同型写像が全単射であるとき，**同型写像**という．$f : R \to S$ が同型写像であるとき，R と S は同型であるといい，$R \cong S$ によって表す．

定義 7.2.1　R が代数的構造をもつとき，R の**自己同型写像**とは同型写像

$\sigma : R \to R$ のことである．R 上の自己同型写像の集合を $\mathrm{Aut}(R)$ で表す．

例 7.2.1 G を位数 n の巡回群とする．g をその生成元とすれば $G = \{1, g, g^2, \ldots, g^{n-1}\}$ と表される．$(k, n) = 1$ ならば，g^k もまた生成元であり，準同型写像

$$\sigma : g \to g^k$$

は G の自己同型写像を定義する．さらに，G の任意の自己同型写像 σ に対して，生成元 g はもう 1 つの生成元 g_1 に写像される．ゆえに，

$$\mathrm{Aut}(G) = \{\sigma\,;\, \sigma : g \to g^k \ (n, k) = 1\}$$

が成り立つ．したがって，$|\mathrm{Aut}(G)| = \varphi(n)$ となる．ここで，$\varphi(n)$ は n より小さくて，n と互いに素である正の整数の個数である[6]． □

例 7.2.2 複素数体 $\mathbb{C}$ を考える．σ を $\mathbb{C}$ の自己同型写像とする．このようなすべての自己同型写像に対して，$\sigma(0) = 0, \sigma(1) = 1, \sigma(-1) = -1$ が成り立つ．したがって，$\sigma(i^2) = (\sigma(i))^2 = -1$. ゆえに，$\sigma(i) = \pm i$ となる．

$\{1, i\}$ は $\mathbb{R}$ 上のベクトル空間 $\mathbb{C}$ の基底であるから，$1, i$ の像は自己同型写像を完全に決定する．したがって，$\mathbb{C}$ にはちょうど 2 つの自己同型写像が存在する．すなわち，それらは次のようである．

$$\begin{aligned} \sigma_1 &: 1 \to 1,\ i \to i, \qquad \text{恒等写像} \\ \sigma_2 &: 1 \to 1,\ i \to -i. \end{aligned}$$

□

例 7.2.3 p を素数として，有限体 $\mathbb{Z}_p$ を考える．このとき，$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ と表され，$\mathbb{Z}_p$ は p を法とする算術的演算をもっている．σ をその自己同型写像とする．$\sigma(1) = 1$ であるから，1 のすべての整数倍に対して $\sigma(n) = n$ が成り立つ．ゆえに，$\sigma(x) = x$ $(x \in \mathbb{Z}_p)$. したがって，$\mathbb{Z}_p$ の自己同型写像はただ 1 つ，恒等写像であり，自己同型群は自明である． □

定理 7.2.1 任意の代数的構造をもつ集合 R に対して，集合 $\mathrm{Aut}(R)$ は写像の合成に関して，R の**自己同型群**と呼ばれる群を構成する．S が R の部分

[6] $\varphi(n)$ をオイラーの関数という．

的代数構造をもつとき，S を**固定**する自己同型写像 $\sigma \in \mathrm{Aut}(R)$, すなわち, $\sigma(s) = s\ (s \in S)$, は部分群をつくる．

例 7.2.4　p を素数とし，G を位数 p の巡回群とする．このとき，$\mathrm{Aut}(G)$ もまた位数 $p-1$ の巡回群であることを示す．

$\mathbb{Z}_p$ を前の例のように位数 p の有限体とする．その加法群は位数 p の巡回群であるから，g を G の生成元とするとき，$1 \to g$ によって定まる同型写像によって $\mathbb{Z}_p$ は G に同型である．$\mathbb{Z}_p$ は体であるから，その 0 でない元は乗法に関して群をつくる．この群を U で表す．

例 7.2.1 によって，G の任意の自己同型写像は生成元の像によって決定される．

$$\sigma : g \to g^k,\ (k, p) = 1.$$

$\mathbb{Z}_p$ の加法群に関する同型写像の言葉では，これは次のものによって与えられる．

$$\sigma : 1 \to k,\ k \neq 0.$$

このとき，この自己同型写像は $\mathbb{Z}_p$ において k 倍することと同じである．したがって，$\mathrm{Aut}(G)$ は $\mathbb{Z}_p$ の乗法群 U に同型である．次に U が巡回群であることを示す．

さて，$|U| = p-1$ であるから，すべての $y \in U$ に対して $y^{p-1} = 1$ が成り立つ．

m を U の元の位数の中で最大のものとすると，$m \leq p-1$ を満たす．$y \in U$ の位数を q とすれば，$q \mid m$ である．ゆえに，$y^q = 1$ であるから $y^m = 1$. したがって，すべての $y \in U$ に対して $y^m = 1$ が成り立つ．以上によって，U の任意の元 y は多項式 $P(x) = x^m - 1$ の根である．$P(x)$ は体上の多項式であるから，高々 m 個の根をもつ．ところが，$P(x)$ は少なくとも $p-1$ 個の根をもつので，$m \geq p-1$ である．ゆえに，$m = p-1$ であり，U は位数が $p-1$ の元をもつ．したがって，U は巡回群である．　□

次に，有限群の部分群の構造について論じよう．G を群とし，H をその部分群とする．G における H の**左剰余類**とは，ある $g \in G$ が存在して，$gH = \{gh; h \in H\}$ と表される集合であった．同様にして，**右剰余類**はある $g \in G$ が存在して，$Hg = \{hg; h \in H\}$ なる集合である．左（右）剰余類の

集合は G を分割し，それぞれの左（右）剰余類は同じ濃度をもつ．だから，左剰余類の個数と右剰余類の個数は同じであることがわかる．この個数は G における H の**指数**と呼ばれ，$|G:H|$ で表される．これらの考えを有限群に適用すると，**ラグランジュの定理**を得る．

定理 7.2.2（ラグランジュの定理）G を有限群とし，H をその部分群とする．このとき，$|G| = |G:H||H|$ が成り立つ．特に，部分群の位数と部分群の指数は共にもとの有限群の位数の約数である．

[歴史的覚え書き] ラグランジュは群という言葉が使われるようになる約 20 年前に亡くなった．実際ラグランジュは，今日我々がラグランジュの定理と呼んでいる定理に同値である置換の閉じた集合についての結果として証明したのである．

例 7.2.5 位数が素数であるすべての有限群は巡回群であることを示す．

p を素数とし，G を位数が p の有限群とする．$x \in G, x \neq 1$ とし，$H = \langle x \rangle$ を x によって生成された巡回部分群とする．ラグランジュの定理によって，H の位数は G の位数の約数である．p は素数だから，$|H| = 1$ かまたは p である．$|H| = 1$ ならば，$x = 1$ となり，$x \neq 1$ と仮定したことに矛盾する．したがって，$|H| = p$ である．このとき，$H = G$ であるから G は巡回群である．

上の議論は，素数位数の有限群は自明でない真の部分群をもたないということも示している． □

さて，次に正規部分群と呼ばれているある特別な種類の部分群を調べよう．この正規部分群によって剰余群を構成することができる．このことは環論においてはイデアルと剰余環との関係に相当する (第 6.2 節参照).

定義 7.2.2 G を群とし，H をその部分群とする．各 $g \in G$ に対して，集合 $g^{-1}Hg$ は H の**共役**と呼ばれる部分群をつくる．$g^{-1}Hg = H$ であるとき，g は H を**正規化**するという．H を正規化する元の集合は G における H の**正規化群**と呼ばれ，$N_G(H)$ によって表される．G のすべての元が H を正規化するとき，すなわち，任意の $g \in G$ に対して $g^{-1}Hg = H$ であるとき，H を G の**正規部分群**といい，$H \lhd G$ により表す．

$H \lhd G$ であるとき，$g^{-1}Hg = H$ が成り立つ．これは $Hg = gH$ を意味している．言い換えると，左剰余類 gH は右剰余類 Hg と同じである．共役，正規化群，正規部分群についての性質を，次の 2 つの補題によってまとめておこう．

補題 7.2.1　次の 4 つの命題は同値である．

(1) $H \lhd G$.

(2) H の G における共役は H ただ 1 つである．

(3) H のすべての左剰余類は右剰余類である．

(4) $N_G(H) = G$.

補題 7.2.2　H を G の部分群とするとき，次が成り立つ．

(1) H の任意の共役は H に同型である．

(2) $N_G(H)$ は G の部分群であり，$H \lhd N_G(H)$.

(3) $|G : N_G(H)|$ は G における H の異なった共役の個数である．

例 7.2.6　アーベル群においては，$g^{-1}Hg = H(g^{-1}g) = H$ であるから，すべての部分群は正規部分群である．

以上続けて見てきた概念の最期のものは**単純群**である．この群は真の自明でない正規部分群をもたない群のことである．たとえば，素数を位数とする巡回群はいかなる真の正規部分群も含まないので単純群である．

単純群は実際有限群を構成しているブロックのようなものであり，有限単純群の広大な理論がある．それらの仕事の多くは**有限単純群の分類定理**と呼ばれているものの証明にかかわっている．この定理はすべての有限単純群の完全なリストを与えている．任意の有限単純群は有限個のよく表現されている群の無限系列のなかの 1 つか，または散在型単純群と呼ばれている有限個の孤立した例の 1 つであることがわかっている．この定理の証明は，現時点においては，2000 ページを越える紙面を必要としている．　□

例 7.2.7　$|G : H| = 2$ ならば，$H \lhd G$ であることを示す．

$g \notin H$ ならば，2 つの剰余類，すなわち $H = 1H$ と gH がある．これらは G を分割するので，

$$G = H \cup gH.$$

これは共通部分のない和集合である．右剰余類に対しても同様の議論により，

$$G = H \cup Hg.$$

これらは共通部分のない和集合であるから，$gH = Hg$, すなわち $g^{-1}Hg = H$ が成り立つ．

これの特別な例として，3 つの文字に関する対称群 S_3 を考察する．例 6.4.1 で $|S_3| = 6$ であることと，位数 3 の元が存在することを見た．ラグランジュの定理によって，この元によって生成された巡回部分群の指数は 2 であり，したがって，正規部分群である．この部分群は 3 個の文字に関する交代群と呼ばれている A_3 である．同様にして，任意の整数 n に対して n 個の文字に関する交代群 A_n と呼ばれている，指数が 2 である S_n の部分群が存在する (しかしながら，$n > 3$ のとき巡回群ではない). A_n は偶置換の全体からなる集合である (演習問題 7.18 参照). □

正規部分群によって剰余群をつくることができる．$H \triangleleft G$ と仮定し，G/H を G における H の剰余類の集合とする．任意の左剰余類は右剰余類でもあるので，左右を特に区別する必要はない．G/H 上に

$$(g_1H)(g_2H) = g_1g_2H$$

という演算を定義することができる．すなわち，$Hg_2 = g_2H$ でかつ $HH = H$ であるから，この演算は矛盾なく定義されて，G/H は群となる．

補題 7.2.3 $H \triangleleft G$ とすれば，G/H は群となる．この群は**剰余群**と呼ばれる．

正規部分群と剰余群は準同型写像と密接な関係をもっている．

定義 7.2.3 $f : G \to G'$ が準同型写像であるとき，f の**核**を $\{g \in G;\, f(g) = 1\}$ によって定義し，$\ker f$ によって表す．f の**像**を $\{g' \in G';\, f(g) = g', \exists g \in G\}$ によって定義し $\mathrm{Im}\, f$ によって表す．

核，像，正規部分群そして剰余群はすべて，第 1 同型定理と呼ばれている次の定理によって結びつけられる．

定理 7.2.3（第 1 同型定理）

(1) $f : G \to G'$ を準同型写像とすれば，$\ker f \lhd G$ であり，Im f は G' の部分群であって，次の同型が成り立つ．

$$G/\ker f \cong \mathrm{Im}\, f.$$

(f が全射であれば，$G/\ker f \cong G'$ であり，G' は f の**準同型像**と呼ばれる．)

(2) $H \lhd G$ ならば，$\ker f = H$, Im $f = G/H$ を満たす準同型写像 $f : G \to G/H$ が存在する．

最後に，代数学の基本定理の証明のために，p が素数として，p-群と p-部分群に関するいくつかの事実が必要となる．

定義 7.2.4　p が素数のとき，p-群とはそのすべての要素の位数が p のベキであるような群 G のことである．G が有限群であれば，G が p-群であるとは，ある自然数 n があって $|G| = p^n$ が成り立つことを意味している．

補題 7.2.4　G が位数 p^n の有限群であるとき，G は位数 p^{n-1} の部分群をもつ．したがって，その部分群の指数は p である．

この補題は p-群に対するラグランジュの定理の逆と考えることができることに注意せよ．ラグランジュの定理は，部分群の位数は全体の群の位数の約数であるということを主張している．それは全体の群の位数の任意の約数に対して，その約数を位数とする部分群が存在することを意味しているわけではない．しかしながら，補題 7.2.4 の 1 つの結果として，すべての p-群に対してこのことは正しい．

系 7.2.1　G が有限 p-群ならば，G の任意の約数に対してその約数を位数とする G の部分群が存在する．

ラグランジュの定理の部分的な逆を与えるシローの定理も必要とする．

定義 7.2.5　G を位数 $|G| = p^m\alpha$ の有限群とする．ここで，p は素数で $(p, \alpha) = 1$ とする．このとき，位数 p^m の部分群のことを **p-シロー部分群**という (G の極大 p-部分群である).

定理 7.2.4 (シローの定理) G を位数 $|G| = p^m\alpha$ の有限群とする．ここで，p は素数で $(p, \alpha) = 1$ である．このとき，次が成り立つ．

(1) G は p-シロー部分群をもつ．

(2) G のすべての p-シロー部分群はすべて共役である．

(3) G のすべての p-部分群はある p-シロー部分群に含まれる．

(4) p-シロー部分群の個数は p を法として 1 に合同であって，かつ $|G|$ の約数であり，したがって α の約数である．

例 7.2.8 位数 12 の群は単純ではないことを示す．

定理 7.2.4 のの結果として，G にただ 1 つの p-シロー部分群しか存在しなければ，それは正規部分群である．今，$|G| = 12 = 2^2 3$ である．ただ 1 つの 2-シロー部分群かまたはただ 1 つの 3-シロー部分群しか存在しないということを示す．

3-シロー部分群の個数は $1 + 3k$ という形をしており，4 の約数である．したがって，ただ 1 つかまたは 4 つの 3-シロー部分群が存在する．ただ 1 つであればそれは正規部分群であるから，4 つの 3-シロー部分群が存在すると仮定する．これらのそれぞれは位数 3 であるから，それらは単位元しか共通部分をもたない．ゆえに，これら 4 つの部分群は G において単位元を除き 8 個の元を含んでいる．

各 2-シロー部分群は 4 個の元をもつ．2-シロー部分群と 3-シロー部分群は単位元しか共通部分をもたない．2 個以上の 2-シロー部分群が存在したと仮定すると，4 個の 3-シロー部分群の中にある 8 個の元の他に付け加えられた 3 個の元が存在することになる．G は 12 個の元しか含んでいないので，これは不可能である．したがって，2-シロー部分群はただ 1 つであるので，それは正規部分群である． □

7.3 ガロア拡大

ガロア理論はある特別な型の有限次代数拡大を扱う．特に，分離性と正規性という 2 つの性質を必要とする．正規性は分離性より単純な性質であるから，最初に議論することにしよう．この章の残りにおいてすべての拡大は有限次拡大を考えることにする．

定義 7.3.1 K は体 F 上の最小分解体であるとき，基礎体 F 上の**正規拡大**という．

正規拡大についてのいくつかの事実は重要である．それらは次の定理の中において与えられる．

定理 7.3.1 K は F の正規拡大とし，$F \subset E \subset K \subset \overline{F}$ と仮定する．ここで，$\overline{F}$ は F の代数的閉包を表す．このとき，次が成り立つ．

(1) F を固定する $\overline{F}$ の任意の自己同型写像は K を K の上に移すので，F を固定する K の自己同型写像である．したがって，$\overline{F}$ のなかの F を固定する K の任意の同型写像は実際 K の自己同型写像である．

(2) K に根をもつ $F[x]$ のすべての既約多項式は K において 1 次因数に分解する．

(3) K は F の正規拡大である．

もう 1 つの重要な性質は分離性である．

定義 7.3.2 α を $f(x)$ の根とする．$f(x) = (x-\alpha)^m g(x)$，$g(\alpha) \neq 0$ のとき，α は**重複度**が m であるという．$m = 1$ のとき，α は**単根**であるといい，そうでないとき，**重根**であるという．

さて，K を F の有限次拡大体とし，$\alpha \in K$ とする．α は $irr(\alpha, F)$ の単根であるとき，**分離的**であるという．K の任意の元が F 上分離的であるとき，K は F の**分離拡大**あるいは K は F 上**分離的**であるという．

以上の定義によって，F の分離拡大において，$\alpha \notin F$ であれば α はその既約多項式の重根ではない．

分離性はガロア拡大に対しては本質的な役割を果たすが，代数学の基本定理において主要な役割を果たすわけではない．それは我々が扱う基礎体は $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ の拡大体だからである．これらの体はすべて標数が 0 であり，この事実よりそれらの拡大体はすべて分離拡大となるからである (第 6.6 節参照)．

定義 7.3.3 $(n)(1) = 0$ を満たす最小の正の整数が n であるとき，体 F の**標数**は n であるという．これを，$\mathrm{char}\, F = n$ と表す．このような n が存在しないとき，F の標数は 0 であるといい，$\mathrm{char}\, F = 0$ と表す．

例 7.3.1 char $\mathbb{Q}$ = char $\mathbb{R}$ = char $\mathbb{C} = 0$ であり，これらの任意の拡大体も標数 0 である．

一方，char $\mathbb{Z}_p = p$ であり，$\mathbb{Z}_p$ の任意の拡大体も標数 p である． □

標数に関する簡単な事実のいくつかをあげておこう．

補題 7.3.1 体の標数は 0 か素数である．

(証明) char $F = n \neq 0$ と仮定する．n が合成数であれば，$n = mk$ ($m < n, k < n$) と表される．このとき，$(n)(1) = (mk)(1) = ((m)(1))((k)(1)) = 0.$ 体は零因子をもたないから，$(m)(1) = 0$ かまたは $(k)(1) = 0$ である．これは n の最小性に矛盾する． ■

補題 7.3.2 char $F = 0$ ならば，F は $\mathbb{Q}$ に同型な体を含んでいる．char $F = p$ ならば，F は $\mathbb{Z}_p$ に同型な体を含んでいる．特に，標数 0 の体は無限集合である．

(証明) 素数標数の場合を示す．標数 0 の場合も同様である．char $F = p$ と仮定する．F は体であるから，単位元 1 を含んでいる．

$E = \{(n)(1); n \in \mathbb{Z}\}$ とおく．char $F = p$ であるから，$E = \{0, 1, (2)(1), \ldots, (p-1)(1)\}$ である．このとき，E から $\mathbb{Z}_p$ への写像 $(k)(1) \to k$ は同型写像である． ■

標数が分離性へ関係してくるのは次の定理である．

定理 7.3.2 標数 0 の体の任意の拡大体は分離拡大である．

実際，有限体の任意の拡大体もまた分離的であるから，分離的でないのは標数 p の無限体の場合のみである．

我々の目的にとって重要なことは，$\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ の任意の拡大は分離的であるという事実である．

分離拡大は次の 2 つの定理によって，体の拡大と群論の間の相互関係にとって本質的である．ここで，後のほうの定理は証明を与える，

定理 7.3.3 K を F の有限次分離拡大とすると，F を固定する K の自己同型写像の個数は有限であり，$[K : F]$ に等しい．

定理 7.3.4（原始元定理）K が F の有限次分離拡大ならば，K は F の単純拡大である．

（証明） K は有限次拡大であるから，K の元 $\alpha_1, \ldots, \alpha_n$ によって $K = F(\alpha_1, \ldots, \alpha_n)$ と表される．帰納法によって，$K = F(\alpha, \beta)$ ならば，ある K の元 γ によって $K = F(\gamma)$ と表されることを示せば十分である．

$n = [K : F]$ とおく．定理 7.3.3 より，F を固定する K の n 個の自己同型写像 $\sigma_1, \ldots, \sigma_n$ が存在する．このとき，次の多項式を考える．

$$p(x) = \prod_{i \neq j} (\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta)).$$

上の式はゼロ多項式ではない．ゆえに，$p(c) \neq 0$ なる元 $c \in K$ が存在[7] する．このとき，元 $\sigma_i(\alpha + c\beta), i = 1, \ldots, n$ は異なっている．したがって，$F(\alpha + c\beta)$ は F 上少なくとも次数は n である．ここで，$F(\alpha + c\beta) \subset F(\alpha, \beta)$ でかつ $F(\alpha, \beta)$ は F 上次数 n である．したがって，$F(\alpha + c\beta) = F(\alpha, \beta)$ でなければならない．

$K = F(\alpha)$ のとき，α を F 上 K の**原始元**という．■

これまでで導入された性質によって，ガロア拡大の定義を与えることができる．

定義 7.3.4 F の有限次で分離的な正規拡大を**ガロア拡大**という．言い換えると，F 上有限次である分離的な最小分解体のことである．

F の標数が 0 のとき，ガロア拡大は単に有限次最小分解体のことである．

F の標数が 0 であると仮定する．このとき，すべての拡大は分離的である．また，$f(x) \in F[x]$ を既約多項式とする．K を F 上 $f(x)$ に対する最小分解体とすれば，K は F のガロア拡大である．K を **$f(x)$ に関する F のガロア拡大**という．

ガロア拡大についてこれまでに知っていることを要約して，この節を閉じることにしよう．

$F \subset E \subset K \subset \overline{F}$ とし，K は F のガロア拡大で，$\overline{F}$ は F の代数的閉包と仮定する．このとき，次のことが成り立っている．

[7] これは K が無限体でないと成立しない．K が有限体のときには，別の理由で K は F の単純拡大となる（参考文献の代数関係の参考書，および訳者による補遺 [3] を参照）．

(1) K は E 上でもガロア拡大である．

(2) F を固定する K の自己同型写像の個数は次数 $[K:F]$ に等しい．

(3) F を固定する $\overline{F}$ のなかの K の任意の同型写像は実際に K の自己同型写像である．

(4) K は F の単純拡大である．

7.4 自己同型写像とガロア群

ガロア群を導入し，群論と体の拡大の間の相互関係を考察しよう．K を F の有限次拡大体であると仮定する．第 7.2 節において，$\mathrm{Aut}(K)$ は群であり，F を固定する $\mathrm{Aut}(K)$ の元はその部分群をつくることを見た．

定義 7.4.1 K を F のガロア拡大とする．F を固定する K の自己同型写像のつくる群を K の F 上のガロア群といい，$\mathrm{Gal}(K/F)$ によって表す．H を $\mathrm{Gal}(K/F)$ の部分群とするとき，H によって動かない K の元の集合を K^H によって表す．

K は F のガロア拡大であるから，分離的であり，定理 7.3.3 より次が成り立つ．

補題 7.4.1 K が F のガロア拡大であるとき，$|\mathrm{Gal}(K/F)| = [K:F]$ が成り立つ．

また K が F のガロア拡大であるとき，その中間体については次の関係がある．

補題 7.4.2 $F \subset E \subset K$ を体の拡大とする．K が F のガロア拡大とするとき，次のことが成り立つ．

(1) K は E のガロア拡大であり，$\mathrm{Gal}(K/E)$ は $\mathrm{Gal}(K/F)$ の部分群である．

(2) H が $\mathrm{Gal}(K/F)$ の部分群ならば，$E = K^H$ は F と K の中間体であり，$\mathrm{Gal}(K/E) = H$ が成り立つ．

（証明） (1) は明らかである．(2) については 3 つのことを示さなければならない．すなわち，K^H は体であること，$F \subset K^H$, そして $\mathrm{Gal}(K/K^H) = H$ が成り立つことである．

$H \subset \mathrm{Gal}(K/F)$ であるから，F のすべての元は H の任意の元によって固定されている．したがって，$F \subset K^H$ である．ゆえに，K^H は空集合ではない．これが体であることを示すには体の演算に関して閉じていることを示さなければならない．

$k_1, k_2 \in K^H$ かつ $\sigma \in H$ と仮定する．このとき，$\sigma(k_1) = k_1, \sigma(k_2) = k_2$ であるから，$\sigma(k_1 \pm k_2) = \sigma(k_1) \pm \sigma(k_2) = k_1 \pm k_2$. ゆえに，$k_1 \pm k_2 \in K^H$. 同様にして，$k_2 \neq 0$ に対して $\sigma(k_1 k_2^{\pm 1}) = \sigma(k_1)\sigma(k_2)^{\pm 1} = k_1 k_2^{\pm 1}$. ゆえに，$k_2 \neq 0$ に対して $k_1 k_2^{\pm 1} \in K^H$ であることが示された．以上より，K^H は F と K の中間体である．

最後に，$E = K^H$ とおく．$\mathrm{Gal}(K/E)$ は E を固定する K の自己同型写像から構成されている．定義によって，E は H の元によって不変な K の元から構成されている．したがって，$\mathrm{Gal}(K/E) = H$ が成り立つ． ■

系 7.4.1 $\mathrm{Gal}(K/F)$ の部分群 H に中間体 K^H を対応させる写像 $\tau : H \to K^H$ は全単射である．

補題 7.4.2 の (1) より，$F \subset E \subset K$ で K を F のガロア拡大とすれば，K は E のガロア拡大である．このとき，どのような条件のもとで E は F のガロア拡大になるであろうか，という問題が自然に発生する．E が F の分離拡大であれば，これは，どのようなときに E は F の正規拡大になるか，という問題になる．この問に対しては，簡潔で優雅な答えがある．すなわち，E が F の正規拡大であるための必要十分条件は $E = K^H$ を満たす $\mathrm{Gal}(K/F)$ の部分群 H が正規部分群になることである．

補題 7.4.3 $F \subset E \subset K$ で K は F のガロア拡大，さらに $E = K^H$ とおく．このとき，E が F のガロア拡大であるための必要十分条件は $H \triangleleft \mathrm{Gal}(K/F)$ となることである．このとき，次の同型が成り立つ．

$$\mathrm{Gal}(E/F) \cong G/H \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

この補題は直接証明することもできるが，次のアルティンの定理を用いて多少簡単に証明することも可能である．

定理 7.4.1（アルティン）K を体として，G を K の自己同型写像のつくる位数 n の有限群とする．このとき，K は $F = K^G$ の有限次ガロア拡大であり，そのガロア群は G である．

（証明） 分離多項式は重根をもたない．α が分離多項式 $f(x)$ の根ならば，$f(x)$ は $irr(\alpha, F)$ で割り切れるので，α は F 上分離的である．

$F = K^G$ でかつ $\alpha \in K$ と仮定する．$g_1, \ldots, g_r \in G$ を $g_1(\alpha), \ldots, g_r(\alpha)$ がすべて異なっているような最大の集合とする．$g \in G$ とすると，g は自己同型写像であり，$\{g_1, \ldots, g_r\}$ は $g_1(\alpha), \ldots, g_r(\alpha)$ がすべて異なる最大の集合だから，$\{gg_1(\alpha), \ldots, gg_r(\alpha)\}$ は $\{g_1(\alpha), \ldots, g_r(\alpha)\}$ の置換である．したがって，α は次の多項式の根である．

$$f(x) = \prod_{i=1}^{r}(x - g_i(\alpha)).$$

さらに，$f(x)$ は任意の $g \in G$ によって不変である．ゆえに，$f(x)$ の係数は $F = K^H$ の中にある．$g_i(\alpha)$ は異なっているので，$f(x)$ は分離的である．したがって，すべての $\alpha \in K$ は F に係数をもつ次数が n 以下の分離多項式の根である．すなわち，K は F の分離拡大である．さらに，$f(x)$ は K で 1 次因数に分解するので，K は正規拡大となる．以上より，K は F のガロア拡大であることがわかる．

K は F の分離拡大であるから，単純拡大である．$K = F(\gamma)$ としよう．ここで，γ は n 次以下の多項式の根であるから，$[K : F] \leq n$. また G は F を固定する K の自己同型写像から構成されているので，$G \subset \mathrm{Gal}(K/F)$ となっている．ゆえに，$[K : F] = |\mathrm{Gal}(K/F)| \geq |G| = n$. したがって，$[K : F] = n$ が成り立ち，かつ G は F 上 K のガロア群である． ■

上に略述した結果はガロア理論の主要な結果である．次の節において，それらを要約しその例を与える．ここでは，多項式のガロア群を調べよう．こことこの節の残りにおいて F は標数 0 であり，したがって，すべての拡大は分離的であることを仮定しよう．

定義 7.4.2 $f(x)$ を F 上の既約多項式で，K を $f(x)$ の最小分解体とする．このとき，K は F のガロア拡大であり，対応しているガロア群を**多項式のガロア群**という．

より詳細にこの多項式のガロア群を調べよう．K を任意の F の代数拡大とする．$\alpha \in K$ として，$irr(\alpha, F)$ をその既約多項式とする．$irr(\alpha, F)$ の他の任意の根 $\overline{\alpha}$ を α の**共役**という．さて，K は F のガロア拡大で，$\sigma \in \mathrm{Gal}(K/F)$ とする．σ は F を固定するので，$irr(\alpha, F) \in F[x]$ も固定する．ゆえに，$\sigma(\alpha)$ は $irr(\alpha, F)$ のもう 1 つの根である．したがって，任意の $\sigma \in \mathrm{Gal}(K/F)$ は元をその共役に写像する．

さて，$f(x) \in F[x]$ を既約とし，その根を $\alpha_1, \ldots, \alpha_n \in K$ とする．$\sigma \in \mathrm{Gal}(K/F)$ とすれば，σ は $f(x)$ を固定し，この根の集合をそれ自身の上に写像する．したがって，次の 2 つの事実がわかった．$\sigma \in \mathrm{Gal}(K/F)$ は既約多項式の根を置換し，また既約多項式の根の共役根もまたその根になる．さらに，次の事実も成り立つ．

補題 7.4.4 K は F のガロア拡大で，$[K:F] = n$ とすれば，$\mathrm{Gal}(K/F)$ は対称群 S_n の部分群である．

$|\mathrm{Gal}(K/F)| = n$ であるから，ケイリーの定理によって，それは置換群であり，したがって S_n の部分群である．重要なことは $\mathrm{Gal}(K/F)$ から，いかにしてその置換が得られるかである．K は F の有限次拡大であるから，適当な元によって $K = F(\alpha_1, \ldots, \alpha_r)$ と表される．$\alpha_1, \ldots, \alpha_r$ を共役元の上に移す置換は自己同型写像を引き起こし，そのガロア群の元を与える．このことを，例でもって説明しよう．

例 7.4.1 $\mathbb{Q}$ 上の $x^4 + 1$ の最小分解体 K を考える．$\mathbb{C}$ において，これは $(x^2 + i)(x^2 - i)$ と分解するので，この多項式は $\mathbb{C}$ で 4 つの根をもつ．

$$\begin{aligned}\omega_1 &= \frac{1+i}{\sqrt{2}} = \sqrt{i}, \quad \omega_2 = \frac{1-i}{\sqrt{2}} = \overline{\omega_1}, \\ \omega_3 &= \frac{-1+i}{\sqrt{2}} = i\omega_1, \ \omega_4 = \frac{-1-i}{\sqrt{2}} = \overline{\omega_3},\end{aligned}$$

ω_1 は 1 の原始 8 乗根であり，$\omega_1^3 = \omega_3$，$\omega_1^5 = \omega_4$，$\omega_1^7 = \omega_2$，$\omega_1^8 = 1$ であることに注意しよう．

したがって，ω_1 は $\mathbb{Q}$ 上 K の原始元であり，$irr(\omega_1, \mathbb{Q}) = x^4 + 1$ かつ $K = \mathbb{Q}(\omega_1)$ である．ゆえに，$[K:\mathbb{Q}] = 4$ となる．次に，ガロア群を調べてみよう．

ω_1 は原始元であるから，自己同型写像 σ は $\sigma(\omega_1)$ によって完全に決定される．ガロア群にはちょうど 4 つの元があり，ω_1 の可能な 4 つの共役元が存在する．ω_1 をそれらの共役元に移すことによって，4 つの異なった自己同型写像が得られる．

$\sigma_1(\omega_1) = \omega_2 = \omega_1^7$ と仮定する．そのとき，$\sigma_2(\omega_2) = \sigma_2(\omega_1^7) = \omega_1^{49} = \omega_1$ である．同様にして，$\sigma_2(\omega_3) = \omega_4, \sigma_2(\omega_4) = \omega_3$ となる．したがって，自己同型写像 σ_2 は次の置換によって与えられる．

$$\omega_1 \to \omega_2,\ \omega_2 \to \omega_1,\ \omega_3 \to \omega_4,\ \omega_4 \to \omega_3.$$

同様の推論によって，残りの自己同型写像はそれぞれ次の置換によって与えられる．

$$\sigma_3\ :\ \omega_1 \to \omega_3,\ \omega_2 \to \omega_4,\ \omega_3 \to \omega_1,\ \omega_4 \to \omega_2.$$

$$\sigma_4\ :\ \omega_1 \to \omega_4,\ \omega_2 \to \omega_3,\ \omega_3 \to \omega_2,\ \omega_4 \to \omega_1.$$

調べてみると，これらの置換のそれぞれは位数が 2 である．このとき，ガロア群 $G = \mathrm{Gal}\ (K/\mathbb{Q})$ は次の表現をもつ．

$$G = \langle \sigma_2, \sigma_3\ ;\ \sigma_2^2 = \sigma_3^2 = (\sigma_2\sigma_3)^2 = 1 \rangle.$$

この群がアーベル群であり，位数 2 の 2 つの有限巡回群の直積である $\mathbb{Z}_2 \times \mathbb{Z}_2$ に同型であることは容易にわかる．この群は通常クラインの 4 元群 (Klein 4-group) と呼ばれている．

ガロア群の構造を調べる別の方法は次のようである．$\omega_1 = \sqrt{i} \in K$ であるから，$i \in K$. ゆえに，$1 + i \in K$ だから $\dfrac{1+i}{\omega_1} = \sqrt{2} \in K$ となる．したがって，$\mathbb{Q}(i, \sqrt{2}) \subset K$ であることがわかる．ここで，$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$ であるから $\mathbb{Q}(i, \sqrt{2}) = K$ を得る．さて，$irr(i, \mathbb{Q}) = x^2 + 1$ より，i の共役元は $\pm i$ であり，一方 $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ より，$\sqrt{2}$ の共役元は $\pm\sqrt{2}$ である．以上より，ガロア群 $\mathrm{Gal}(K/\mathbb{Q})$ における 4 つの可能な自己同型写像は次のように与

えられる．

$$\begin{aligned}
&\sigma_1 : i \to i,\ \sqrt{2} \to \sqrt{2} \qquad \text{恒等写像}\\
&\sigma_2 : i \to -i,\ \sqrt{2} \to \sqrt{2}\\
&\sigma_3 : i \to i,\ \sqrt{2} \to -\sqrt{2}\\
&\sigma_4 : i \to -i,\ \sqrt{2} \to -\sqrt{2}.
\end{aligned}$$

ここで，各自己同型写像が位数 2 であることは容易にわかる．　□

7.5　ガロア理論の基本定理

最期の 2 つの節の結果を，ガロア理論の基本定理と呼ばれている 1 つの定理のなかに要約する．それから，その定理のいくつかの応用，そして次の 2 つの節において，代数学の基本定理の第 4 番目の証明を与える．

定理 7.5.1（ガロア理論の基本定理）K を F のガロア拡大とし，そのガロア群を $G = \mathrm{Gal}(K/F)$ とする．中間体 E に対して，$\tau(E)$ を E を固定する G の部分群とする．このとき，次が成り立つ．

(1) τ は F を含んでいる中間体の集合と G の部分群の集合との間の全単射である．

(2) H が G の部分群でかつ $E = K^H$ ならば，$\tau(E) = H$ である．

(3) K は E のガロア拡大であり，$\mathrm{Gal}(K/E) = \tau(E)$ が成り立つ．

(4) $|G| = [K : F]$.

(5) $[E : F] = |G : \tau(E)|$. すなわち，基礎体上の中間体の次数はガロア群において，対応している部分群の指数に等しい．

(6) E が F 上ガロア拡大であるための必要十分条件は $\tau(E) \lhd G$ なることである．このとき，次の同型がある．

$$\mathrm{Gal}(E/F) \cong G/\tau(E) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E).$$

(7) F を含んでいる K の部分体の束はガロア群の部分群のつくる逆束になっている．

(1) から (6) はすでに考察した．(7) について少し述べてみよう．F 上 K の部分体のつくる束によって，中間体すべての集合とそれらの間の相互関係を意味するものとする．部分群の束についても同様である．体のほうにおいて，E を部分体とするとき，次数 $[K:E]$ は $\mathrm{Gal}(K/E)$ の位数であり，一方その指数は $[E:F]$ である．したがって，部分体の集合はその束において上からの順序であり，他方部分群の集合である束においては下からの順序である．すなわち，自明な群を $\mathrm{Gal}(K/K)=\{1\}$ とすれば次の図式で表せる．

$$
\begin{array}{ccc}
K & \longleftrightarrow & \mathrm{Gal}(K/K) \\
\cup & & \cap \\
E & \longleftrightarrow & \mathrm{Gal}(K/E) \\
\cup & & \cap \\
F & \longleftrightarrow & \mathrm{Gal}(K/F)
\end{array}
$$

次にあげる 3 つの例によって，上記のことを説明する．

例 7.5.1 x^4+1 の $\mathbb{Q}$ 上の最小分解体を考える．例 7.4.1 で見たように，$K=\mathbb{Q}(i,\sqrt{2})$ である．このとき，$[K:\mathbb{Q}]=4$ でありそのガロア群は $\mathbb{Z}_2\times\mathbb{Z}_2$ である．$\mathrm{Gal}(K/\mathbb{Q})$ における 4 つの自己同型写像は次のようなものであった．

$$
\begin{aligned}
1 &: i \to i,\ \sqrt{2}\to\sqrt{2} \\
\sigma &: i \to i,\ \sqrt{2}\to-\sqrt{2} \\
\tau &: i \to -i,\ \sqrt{2}\to\sqrt{2} \\
\sigma\tau &: i \to -i,\ \sqrt{2}\to-\sqrt{2}.
\end{aligned}
$$

これらの各元は位数 2 であり，したがって $\mathrm{Gal}(K/\mathbb{Q})$ の部分群は全部で 5 個ある．それらは次のようである．

$$\{1\},\ H_1=\{1,\tau\},\ H_2=\{1,\sigma\tau\},\ H_3=\{1,\sigma\},\ G.$$

これらに対応している 5 個の中間体を示そう．G の不変体はちょうど $\mathbb{Q}$ となり，一方，$\{1\}$ の不変体は K である．さて，H_3 を考えよう．$i\in K$ でか

つ $\mathbb{Q}(i) \subset K, [K : \mathbb{Q}(i)] = 2$ であるから，$\mathbb{Q}(i)$ は指数 2 の部分群に対応している．ゆえに，その部分群の位数は 2 である．σ は i を固定し，$\sqrt{2}$ はそうではない．ゆえに，σ は $\mathbb{Q}(i)$ を固定するが，K のすべての元を固定するわけではない．したがって，H_3 の不変体は $\mathbb{Q}(i)$ である．

同様に，$\mathbb{Q}(\sqrt{2}) \subset K$ であり，そのとき，$\mathbb{Q}(\sqrt{2})$ は H_1 の不変体である．

最後に，$i, \sqrt{2} \in K$ であるから，$i\sqrt{2} \in K$. ゆえに，$\mathbb{Q}(i\sqrt{2}) \subset K$ である．$irr(i\sqrt{2}, \mathbb{Q}) = x^2 + 1$ だから，$[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$ となる．自己同型写像 $\sigma\tau$ は $i\sqrt{2}$ を固定する．ゆえに，$\mathbb{Q}(i\sqrt{2})$ は H_2 の不変体である．これらの関係を図 7.1 と図 7.2 で説明する．□

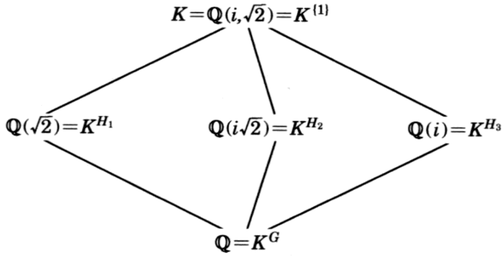


図 7.1　部分体の束

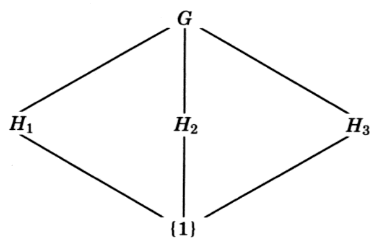


図 7.2　部分群の束

例 7.5.2　$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とする．これは $(x^2 - 2)(x^2 - 3)$ の $\mathbb{Q}$ 上の最小分解体であるから，K は $\mathbb{Q}$ のガロア拡大である．$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ でかつ $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ であるから，$[K : \mathbb{Q}] = 4$. そのガロア群は次の 4 つの自己同型写

像によって表現される.

$$1: \sqrt{2} \to \sqrt{2},\ \sqrt{3} \to \sqrt{3}$$
$$\sigma: \sqrt{2} \to \sqrt{2},\ \sqrt{3} \to -\sqrt{3}$$
$$\tau: \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to \sqrt{3}$$
$$\sigma\tau: \sqrt{2} \to -\sqrt{2},\ \sqrt{3} \to -\sqrt{3}.$$

この群は $\mathbb{Z}_2 \times \mathbb{Z}_2$ であり，前出の例のガロア群と同型であることが容易にわかる．したがって，同じ基礎体上の異なった拡大体でも同型なガロア群をもつことがあり得る．対応している部分群と不変体は次のようである．

$$\begin{aligned}
&H_0 = \{1\} &&\Rightarrow \text{不変体は } K = \mathbb{Q}(\sqrt{2}, \sqrt{3}),\\
&H_1 = \{1, \sigma\} &&\Rightarrow \text{不変体は } \mathbb{Q}(\sqrt{2}),\\
&H_2 = \{1, \tau\} &&\Rightarrow \text{不変体は } \mathbb{Q}(\sqrt{3}),\\
&H_3 = \{1, \sigma\tau\} &&\Rightarrow \text{不変体は } \mathbb{Q}(\sqrt{2}\sqrt{3}) = \mathbb{Q}(\sqrt{6}),\\
&H_4 = G &&\Rightarrow \text{不変体は } \mathbb{Q}.
\end{aligned}$$
□

例 7.5.3 もう少し複雑な例として，$x^4 - 2$ の $\mathbb{Q}$ 上の最小分解体 K を考えよう．

$\mathbb{C}$ において，$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ であるから，$\omega = 2^{1/4}$ とおけば，4 つの根は ω, $i\omega$, $-\omega$, $-i\omega$ である．したがって，$i\omega/\omega = i \in K$ より $\mathbb{Q}(i, \omega) \subset K$ となる．ところが，$x^4 - 2$ は $\mathbb{Q}(i, \omega)$ において 1 次因数に分解するので $K = \mathbb{Q}(i, \omega)$ となる．

さて，$\mathbb{Q}(\omega)$ は $\mathbb{Q}$ 上の次数は 4 であり，$\omega \in \mathbb{R}$ より $i \notin \mathbb{Q}(\omega)$ である．ゆえに，$[K : \mathbb{Q}(\omega)] = 2$ である．K は $\mathbb{Q}(\omega)$ に i を添加した体であるから，$[K : \mathbb{Q}] = 8$ となる．

ω の 4 つの共役元は ω, $i\omega$, $-\omega$, $-i\omega$ であり，一方 i の共役元は $\pm i$ であ

る．したがって，Gal$(K/\mathbb{Q})$ における 8 個の自己同型写像は次のようである．

$$1 : \omega \to \omega,\ i \to i$$
$$\sigma : \omega \to i\omega,\ i \to i$$
$$\sigma^2 : \omega \to -\omega,\ i \to i$$
$$\sigma^3 : \omega \to -i\omega,\ i \to i$$
$$\tau : \omega \to \omega,\ i \to -i$$
$$\sigma\tau : \omega \to i\omega,\ i \to -i$$
$$\sigma^2\tau : \omega \to -\omega,\ i \to -i$$
$$\sigma^3\tau : \omega \to -i\omega,\ i \to -i$$

簡単な計算によって，$\sigma^4 = 1,\ \tau^2 = 1$ かつ $\sigma\tau = \tau\sigma^3$ であることがわかる．この群は正方形のシンメトリーを表している位数 8 の 2 面体群 D_4 である．この群の表現は次のようである．

$$D_4 = \langle \sigma, \tau\ ;\ \sigma^4 = 1,\ \tau^2 = 1,\ \sigma\tau = \tau\sigma^3 \rangle.$$

D_4 には全部で 10 個の部分群がある．

$H_1 = \{1\}$ ⇒ 不変体は $K = \mathbb{Q}(i, \omega)$,
$H_2 = \{1, \sigma, \sigma^2, \sigma^3\}$ ⇒ 不変体は $\mathbb{Q}(i)$,
$H_3 = \{1, \sigma^2\}$ ⇒ 不変体は $\mathbb{Q}(i, \sqrt{2})$,
$H_4 = \{1, \tau\}$ ⇒ 不変体は $\mathbb{Q}(\omega)$,
$H_5 = \{1, \sigma\tau\}$ ⇒ 不変体は $\mathbb{Q}(\omega + i\omega)$,
$H_6 = \{1, \sigma^2\tau\}$ ⇒ 不変体は $\mathbb{Q}(i\omega)$,
$H_7 = \{1, \sigma^3\tau\}$ ⇒ 不変体は $\mathbb{Q}(\omega - i\omega)$,
$H_8 = \{1, \sigma^2, \tau, \sigma^2\tau\}$ ⇒ 不変体は $\mathbb{Q}(\sqrt{2})$,
$H_9 = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$ ⇒ 不変体は $\mathbb{Q}(i\sqrt{2})$,
$H_{10} = D_4$ ⇒ 不変体は $\mathbb{Q}$. □

7.6 代数学の基本定理——証明 4

さて，代数学の基本定理の第 4 の証明を与えるところまでやってきた．この証明はこれまでの節において組織的に構成してきたガロア理論を用いる．

定理 7.6.1（代数学の基本定理）複素数体は代数的閉体である．すなわち，任意の定数でない複素多項式は $\mathbb{C}$ において根をもつ．

（証明） $f(x) \in \mathbb{C}[x]$ とすると，$f(x)$ の $\mathbb{C}$ 上の最小分解体 K を考えることができる．これは $\mathbb{C}$ のガロア拡大であり，$\mathbb{C}$ は $\mathbb{R}$ の有限次拡大体であるから，K は $\mathbb{R}$ のガロア拡大である．代数学の基本定理は K が $\mathbb{C}$ 自身であるということを主張している．したがって，代数学の基本定理は $\mathbb{C}$ の任意の自明でないガロア拡大は $\mathbb{C}$ でなければならないという事実と同値である．

K を $\mathbb{R}$ の任意の有限次拡大体で，$[K:\mathbb{R}] = 2^m q$, $(2,q) = 1$ とする．$m = 0$ ならば，K は $\mathbb{R}$ の奇数次の拡大体である．K は $\mathbb{R}$ 上分離的であるから，それは単純拡大である．ゆえに，$K = \mathbb{R}(\alpha)$ と表され，$irr(\alpha,\mathbb{R})$ は奇数次の次数をもつ．ところが，奇数次の実多項式は常に実数の根をもつ．したがって，$irr(\alpha,\mathbb{R})$ はその次数が 1 であるときにのみ既約である．このとき，$\alpha \in \mathbb{R}$ であるから $K = \mathbb{R}$ となる．ゆえに，K は $\mathbb{R}$ の自明でない拡大であれば，$m > 0$ である．このことは，より一般的に $\mathbb{R}$ のいかなる奇数次の有限次拡大も存在しないことを示している．

K を $\mathbb{C}$ の次数 2 の拡大体とする．このとき，$K = \mathbb{C}(\alpha)$ で $irr(\alpha,\mathbb{C}) = 2$ である．ここで，複素 2 次多項式は $\mathbb{C}$ に根をもつので，矛盾である．したがって，$\mathbb{C}$ は次数 2 の拡大をもたない．

次に，K を $\mathbb{C}$ のガロア拡大体とする．K は $\mathbb{R}$ 上でもガロア拡大である．$[K:\mathbb{R}] = 2^m q, (2,q) = 1$ と仮定する．上でなされた議論より，$m > 0$ でなければならない．$G = \mathrm{Gal}(K/\mathbb{R})$ をそのガロア群とする．そのとき，$|G| = 2^m q$, $m > 0$, $(2,q) = 1$ である．したがって，G は位数 2^m で指数 q の 2-シロー群をもつ．この群は $[K:E] = 2^m$, $[E:\mathbb{R}] = q$ を満たす中間体 E に対応している．しかしながら，E は $\mathbb{R}$ の奇数次の有限次拡大体である．ゆえに，$q = 1$, $E = \mathbb{R}$ となり，$[K:\mathbb{R}] = 2^m$, $|G| = 2^m$ を得る．

さて，$[K:\mathbb{C}] = 2^{m-1}$ であって，$G_1 = \mathrm{Gal}(K/\mathbb{C})$ とおく．これは 2-群である．もし，この群が自明でなければ，補題 7.2.4 より，位数 2^{m-2} で指数 2

の部分群が存在する．この部分群は $\mathbb{C}$ 上の次数が 2 である中間体に対応する．しかしながら，上の議論より $\mathbb{C}$ は次数 2 の拡大をもたない．したがって，G_1 は自明である．すなわち，$|G_1| = 1$ であり，ゆえに，$[K : \mathbb{C}] = 1$ でかつ $K = \mathbb{C}$ となる．これより，証明は完結した． ■

前の証明においては，より一般的な結果を実際に証明した．上記の証明では，ガロア理論のほかに 2 つの事実を用いた．すなわち，奇数次の実多項式は常に実数の根をもつということと，次数 2 の複素多項式は複素数の根をもつという事実である．性質として，これら 2 つの事実を使えば次の一般化を証明することができる．

定理 7.6.2 K をその中ですべての正の数が平方根をもつような順序体とする．さらに，$K[x]$ における奇数次の多項式は K において根をもつと仮定する．このとき，$K(i)$ は代数的閉体である．ただし，$i = \sqrt{-1}$ は既約多項式 $x^2 + 1 \in K[x]$ の根である．

7.7　ガロア理論のいくつかの応用

ガロア理論は最初 5 次多項式のベキ根による不可解性の証明を扱うために発展した．この節においては，この証明を概観してみよう．第 1 章で述べたように，ベキ根による可解性の問題は長く，そして興味ある歴史をもっている．2 次方程式を解く能力と，2 次方程式の根の公式の本質は 3600 年前のバビロニア人によって知られていた．2 次方程式の根の公式は，虚数の発見によって，$\mathbb{C}$ 上任意の 2 次多項式は $\mathbb{C}$ において根をもつということになる．16 世紀にイタリア人の数学者タルターリャは 3 次方程式を解くためのベキ根による同様な公式を発見した．この 3 次方程式の根の公式は今日，1545 年にカルダノがはじめて発表した（実際は誤りである）として，**カルダノの公式**という名で知られている．この公式の初期の特別な形はフェッロによって発見されていた．カルダノの弟子のフェラーリは，この公式を 4 次の多項式に対するベキ根による根の公式に発展させた．

カルダノから 19 世紀の初頭まで，5 次の多項式に対する同様の公式を得ようとする試みがなされた．1805 年にルフィニは，5 次の多項式は一般にベ

キ根によって解くことは不可能であることを証明[8]した．したがって，5 次の多項式に対してはそれ以下の次数の多項式に対するような公式は存在しない．アーベルは 1825 年〜1826 年に，ガロアは 1831 年に，ルフィニの結果を発展させ，一般の 5 次あるいはそれ以上の多項式に対するベキ根による不可解性を証明した．

ガロア理論を適用するに際して，ベキ根による不可解性を群論の性質，すなわち，対応しているガロア群が満たしていなければならない性質に翻訳しなければならない．

定義 7.7.1 群 G は次のような部分群の有限な列をもつとき，**可解群**であるという．

$$G = G_1 \supset G_2 \supset G_3 \supset \cdots \supset G_n = 1.$$

ここで，$G_{i+1} \triangleleft G_i$ かつ G_i/G_{i+1} はアーベル群である．このような列を G に対する**正規列**といい，G_i/G_{i+1} を正規列の**因子群**という．このとき，上の定義は正確に次のように置き換えることができる．群 G は可換な因子群をもつ正規列が存在するとき，可解群である．

可解群の族は部分群，剰余群そして有限個の直積に関して閉じていることが示される．すなわち，G, H が可解群ならば，G または H の部分群，G または H の剰余群，そして，直積 $G \times H$ がまた可解群になることが証明される．

さて，ベキ根による可解性は体の拡大の概念によってどう表されるのか明確にしなければならない．

定義 7.7.2 K が**ベキ根による** F **の拡大**であるとは，適当な元 $\alpha_1, \ldots, \alpha_r$ と適当な整数 $n_1, \ldots, n_r$ が存在して，$K = F(\alpha_1, \ldots, \alpha_r)$ であって，$\alpha_1^{n_1} \in F$, $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ $(i = 2, \ldots, r)$ を満たすことである．

多項式 $f(x) \in F[x]$ が F 上**ベキ根によって可解**であるとは，$f(x)$ の最小分解体がベキ根による F の拡大になっていることである．

---

[8] いくつかの文献によればルフィニの証明は完全なものではなかった（たとえば，参考文献の「訳者による補遺」[2][4] を参照してほしい）．

これら 2 つの概念－群の可解性とベキ根による可解性－を結びつける鍵となる結果は次の定理である．

定理 7.7.1 K を $\mathrm{char}\, F = 0$ である F のガロア拡大とする．このとき，K がベキ根による F の拡大ならば，$\mathrm{Gal}(K/F)$ は可解群である．

したがって，一般に次数が 5 またはそれ以上大きい多項式を解くことが不可能であることを示すためには，任意の $n \geq 5$ に対して，そのガロア群が可解でない次数 n の多項式が存在することを示さねばならない．ガロア群は常に，適当な対称群の中に含まれ，そして次の定理が成り立っている．

定理 7.7.2 任意の $n \geq 5$ に対して，対称群 S_n は可解群ではない．

この定理によって，任意の n に対して，そのガロア群が全体の対称群 S_n である多項式の存在を示せばベキ根による不可解性を示すことができるであろう．これは次のように示すことができる．

$y_1, \ldots, y_n$ を $\mathbb{Q}$ 上独立な超越元とし，$K = \mathbb{Q}(y_1, \ldots, y_n)$ とおく．$s_1, \ldots, s_n$ を $y_1, \ldots, y_n$ の基本対称式として (第 6.4 節参照)，$F = \mathbb{Q}(s_1, \ldots, s_n)$ とおく．このとき，K は F のガロア拡大で $\mathrm{Gal}(K/F) \cong S_n$ となっている．

定理 7.7.3 $y_1, \ldots, y_n$ を $\mathbb{Q}$ 上独立な超越元とする．このとき，多項式 $f(x) = \prod_{i=1}^{n}(x - y_i)$ は $F = \mathbb{Q}(s_1, \ldots, s_n)$ 上ベキ根によって可解ではない．ただし，$s_1, \ldots, s_n$ は $y_1, \ldots, y_n$ の基本対称式である．

最後の応用として，幾何学的な定規とコンパスによる作図問題の不可能性に注意を向けよう．古代におけるギリシャの数学者達は定規とコンパスのみを用いて，立方体の 2 倍の体積をもつ立方体をつくること（立方体倍積問題），角を 3 等分すること（角の 3 等分問題），与えられた円と等積の正方形をつくること（円積問題）が作図可能かという問題を提出した．ギリシャ人達は，このような作図が不可能であることを証明できなかった．彼らができたのは円錐曲線の切り口を含めて，他の方法を用いてのみこれらの問題に対する解答を与えることができるということであった．1837 年に，ワンツェルは代数的な方法を用いて，角の 3 等分問題と立方体倍積問題が不可能であることを

証明することができた．円周率 π が超越的であることの証明 (1882 年にリンデマンによって証明された．第 6.6 節参照) とともに，ワンツェルの方法は円積問題もまた不可能であるということを示すために応用することができた．その代数的な方法の要点を述べよう．5 次方程式の不可解性のときのように，上の問題を体の拡大の言葉に翻訳しなければならない．まず最初に，**作図可能数**を定義する．

定義 7.7.3　単位長さの線分が与えられていると仮定する．$\alpha \in \mathbb{R}$ は，定規とコンパスを用いて，単位線分から有限回の操作で長さ $|\alpha|$ の線分をひくことができるとき**作図可能**であるという．

初等的な幾何学から，定規とコンパスを用いて次のようなことが可能であるということを思い出そう．与えられた点を通り与えられた線分に平行な直線をひくこと，与えられた線分をのばすこと，与えられた直線上の任意の点においてその直線に対して垂線をひくことなどがある．最初の定理はすべての作図可能な数の集合は $\mathbb{R}$ の部分体をなすという結果である．

定理 7.7.4　すべての作図可能な数の集合 C は $\mathbb{R}$ の部分体をなす．さらに，$\mathbb{Q} \subset C$ が成り立つ．

(**証明**)　C をすべての作図可能な数の集合とする．与えられた単位長さの線分は作図可能であるから，$1 \in C$ である．ゆえに，$C \neq \emptyset$. したがって，C が体であることを示すためには体の演算に関して閉じていることを示さなければならない．

α, β が作図可能であると仮定する．このとき，$\alpha \pm \beta, \alpha\beta, \alpha/\beta\ (\beta \neq 0)$ が作図可能であることを示さなければならない．$\alpha, \beta > 0$ のとき，長さ $|\alpha|$ の線分をひく．この線分の一方の端点から長さ $|\beta|$ の線分をひく．このようにして，長さ $\alpha + \beta$ の線分を作図したことになる．同様に，$\alpha > \beta$ のとき，長さ $|\alpha|$ の線分上で最初から長さ $|\beta|$ の線分をひくと，残った部分が $\alpha - \beta$ となる．場合分けを考えると，α または β あるいは 2 つとも負の場合にも，同様にして上のような考察をすることができる．この作図は図 7.3 において示されている．したがって，$\alpha \pm \beta$ は作図可能である．

図 7.4 に $\alpha\beta$ を作図する仕方を示してある．線分 $\overline{OA}$ の長さを $|\alpha|$ とする．O を通り $\overline{OA}$ と一致しない直線 L をひく．直線 L 上に長さ β の線分を $\overline{OB}$



図 7.3　$\alpha \pm \beta$ の作図可能性

とする．$\overline{OP}$ の長さが 1 となるように P, B を通る直線上に点 P をとる．次に，O, A を通る直線上に $\overline{BQ}$ が $\overline{AP}$ に平行になるように点 Q をとる．相似三角形であることより，次のことがわかる．

$$\frac{|\overline{OP}|}{|\overline{OB}|} = \frac{|\overline{OA}|}{|\overline{OQ}|} = \frac{|\alpha|}{|\overline{OQ}|}.$$

そのとき，$|\overline{OQ}| = |\alpha||\beta|$ であるから $\alpha\beta$ は作図可能である．

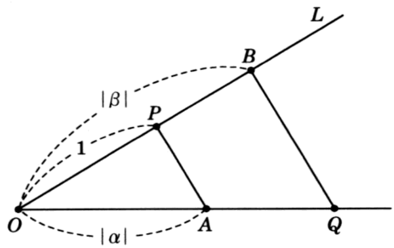


図 7.4　$\alpha\beta$ の作図可能性

図 7.5 に示されているように，上の例と同様な作図によって α/β $(\beta \neq 0)$ が作図可能であることが示される．$\overline{OA}, \overline{OB}, \overline{OP}$ を上の例と同じにとる．A と B を結び，$\overline{PQ}$ を $\overline{AB}$ に平行にとる．再び相似三角形であることより，次のことがわかる．

$$\frac{1}{|\beta|} = \frac{|\overline{OQ}|}{|\alpha|} \Rightarrow \frac{|\alpha|}{|\beta|} = |\overline{OQ}|.$$

ゆえに，α/β は作図可能である．

以上より，C は $\mathbb{R}$ の部分体である．$\mathrm{char}(C) = 0$ であるから，$\mathbb{Q} \subset C$ がわかる．■

次に，作図可能数は平面においてどのように構成されるかを分析してみよう．原点から出発して，単位長さと上で考察した構成法を用いて，平面において有理数の座標をもつ任意の点を特定しよう．すなわち，$q_1, q_2 \in \mathbb{Q}$ として，

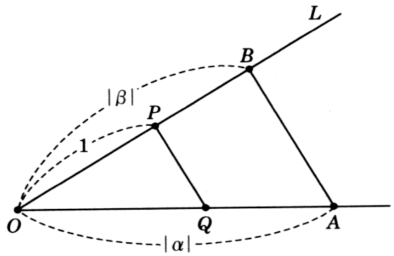


図 7.5 α/β の作図可能性

点 $P = (q_1, q_2)$ を作図することができる．定規とコンパスのみを用いて，平面における作図可能な点は次の 3 つの方法のうちの 1 つによって決定される．

(1) 2 つの直線の交点．それらの各直線は与えられた有理数の座標をもつ 2 つの点を通る直線である．

(2) 直線と円の交点．直線は与えられた有理数の座標をもつ 2 つの点を通る直線であり，円は，その中心が有理数の座標をもち，半径の 2 乗が有理数である．

(3) 2 つの円の交点．それぞれの円は，中心が有理数の座標をもち，半径は有理数の平方根である．

分析すると，最初の場合は有理数係数の 2 つの 1 次方程式の解であることを意味しているので，その解は有理数である．2 番目と 3 番目の場合は $x^2 + y^2 + ax + by + c = 0$ $(a, b, c \in \mathbb{Q})$ の形の方程式を解かなければならない．これらは $\mathbb{Q}$ 上の 2 次方程式であり，したがって，その解は $\mathbb{Q}$ に属しているかまたは $\mathbb{Q}$ の 2 次拡大 $\mathbb{Q}(\sqrt{\alpha})$ に属している．1 度 $\mathbb{Q}$ の 2 次拡大が見つけられれば，その操作は繰り返すことができる．逆に，α が作図可能であれば，$\sqrt{\alpha}$ も作図可能である．以上のようにして，次の定理を証明することができる．

定理 7.7.5 $\gamma \notin \mathbb{Q}$ が作図可能ならば，有限個の実数 $\alpha_1, \ldots, \alpha_r \in \mathbb{R}, \alpha_r = \gamma$ が存在して，各 i $(i = 1, \ldots, r)$ に対して $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ は $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ の 2 次拡大体である．特に，適当な $n \geq 1$ に対して $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^n$ が成り立つ．

したがって，作図可能数の集合は $\mathbb{Q}$ から 2 次拡大体を繰り返して得られる．この考えを用いて，前に述べた 3 つの作図問題の不可能性を示そう．

例 7.7.1 立方体を 2 倍にする（立方体倍積問題）ことは不可能である．これは次のことを意味している．一辺の長さが与えられた立方体に対して，定規とコンパスを用いて，もとの立方体の体積の 2 倍の体積をもつ立方体をつくることは不可能である．

与えられた一辺の長さが 1 であるとき，もとの立方体の体積は 1 である．これを 2 倍にするには，長さ $2^{1/3}$ の辺を作図しなければならない．ところが，$irr(2^{1/3}, \mathbb{Q}) = x^3 - 2$ であるから $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ となり，これは 2 のベキではない．したがって，$2^{1/3}$ は作図可能ではない．□

例 7.7.2 角の 3 等分は不可能である．これは次のことを意味している．任意に与えられた角を定規とコンパスのみを用いて 3 等分することは不可能である．

角 θ が作図可能であるための必要十分条件は長さ $\cos\theta$ の線分が作図可能なることである．たとえば，$\cos(\pi/3) = 1/2$ であるから，$\pi/3$ は作図可能である．定規とコンパスだけで 3 等分することはできないことを示す．

三角関数の次の等式がある．

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

$\alpha = \cos\dfrac{\pi}{9}$ とおく．上の等式より $4\alpha^3 - 3\alpha - \dfrac{1}{2} = 0$. 多項式 $4x^3 - 3x - \dfrac{1}{2}$ は $\mathbb{Q}$ 上既約であるから，$irr(\alpha, \mathbb{Q}) = 4x^3 - 3x - \dfrac{1}{2}$. ゆえに，$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. したがって，$\alpha$ は作図不可能である．それゆえ，対応している角 $\pi/9$ は作図不可能である．以上より，$\pi/3$ は作図可能であるが，3 等分はできない．□

例 7.7.3 円を正方形にする（円積問題）ことは不可能である．これは次のことを意味している．与えられた円に対して，定規とコンパスのみを用いて，与えられた円の面積と等しい面積をもつ正方形を作図することは不可能である．

与えられた円の半径が 1 であると仮定する．これは作図可能であり，面積は π である．対応する正方形の一辺の長さは $\sqrt{\pi}$ でなければならない．ところが π は超越数である．したがって，π は作図不可能である．□

ガロア理論によって解決された大きな他の作図問題は正 n 角形の作図である．$n \geq 3$ に対して，正 n 角形が作図可能であるための必要十分条件は $2\pi/n$

が作図可能なることである．さらに，このことは $\cos(2\pi/n)$ が作図可能であることと同値である．正 n 角形の作図可能性についての代数的研究は 19 世紀の初期にガウスによって始められた．

7.8 ℝ の代数拡大と結論

F を実数 $\mathbb{R}$ の有限次代数拡大体とする．代数学の基本定理の証明から，$F = \mathbb{R}$ かまたは，$[F : \mathbb{R}] = 2$ かつ $F \cong \mathbb{C}$ である．したがって，代数学の基本定理は次のように表現することもできる．

定理 7.8.1 F を実数 $\mathbb{R}$ の有限次代数拡大体とする．このとき，$[F : \mathbb{R}] > 1$ ならば $[F : \mathbb{R}] = 2$ かつ $F \cong \mathbb{C}$ である．

体の定義を少し拡張すればさらに実数の拡大体を分類することができる．**division ring** とは体と同じ性質をもっているが，乗法が必ずしも可換でない代数的構造をもつ集合である．すなわち，それは単位元をもち，すべての 0 でない元は乗法逆元をもつ環のことである．したがって，すべての体は division ring であるが，以下において見るように非可換な division ring が存在する．非可換な division ring は**斜体**と呼ばれる．F を体とする．F を含んでいる division ring D は F 上のベクトル空間である．さらに，D にはすべての 0 でない元は乗法逆元をもつという乗法がある．F における単位元は division ring の単元である．このとき，D は F 上の **多元体**と呼ばれる．ここで，F の元は D のすべての元と可換である．

斜体を構成する方法を考える．F は体で，そこにおいては，いかなる平方の和も 0 にならないと仮定する．すなわち，$x_1^2 + \cdots + x_n^2 = 0$ $(x_1, \ldots, x_n \in F)$ ならば $x_i = 0$ $(i = 1, \ldots, n)$ となっている．この性質を満たす体は **totally real field** と呼ばれている．さて，基底を $1, i, j, k$ とする F 上の次元 4 のベクトル空間 H_F を考える．1 は F の単位元と同一視して，基底の間の積を定義することによって H_F 上に乗法を定める．$i^2 = j^2 = k^2 = -1$, $ijk = -1$ とする．これによって，結合律を使えば基底の間のすべての積を完全に定義することができる．たとえば，$ijk = -1, k^2 = -1$ より $ij = -k^{-1} = k$ を得る．すると，$ik = i(ij) = (ii)j = -j$ である．$ij = -ji$ であることは容易に確かめられるので，この積は非可換である．

ベクトル空間 H_F の一般的な元は $f_0+f_1i+f_2j+f_3k$ という形をしている．このような元の乗法は定義されている基底の積を用い，代数的操作によって行われる．以上のようにして，H_F 上に積が定義される．直接計算することによって，次の定理を証明することができる．

定理 7.8.2 totally real field F に対して，H_F は F 上次元 4 の多元体をつくる．H_F を F 上の **4 元数体**という．

上の証明のなかで難しいのは逆元の存在だけである．この証明は複素数のときと同じようになされるので，演習問題として残しておく．

ハミルトンの 4 元数体 H は実数体上の 4 元数体である．すなわち，$H=H_{\mathbb{R}}$ である．この環は $r_0+r_1i+r_2j+r_3k$ $(r_i\in\mathbb{R})$ という形の元から構成されている．$\mathbb{R}$ を第 1 の成分と同一視すれば $\mathbb{R}\subset H$ である．したがって，H は $\mathbb{R}$ の有限次斜体拡大である．次の定理はこの拡大がただ 1 つであることを示している．

定理 7.8.3 D を $\mathbb{R}$ 上の次数が 1 より大きい有限次元の多元体とする．D が体であれば，$[D:\mathbb{R}]=2$ かつ $D\cong\mathbb{C}$ である．また，D が斜体であれば，$[D:\mathbb{R}]=4$ かつ $D\cong H$ となる．

（証明） D が体であれば，代数学の基本定理を言い換えただけなので，D が斜体である場合を考える．以下にその証明の概要を説明し，その詳細は演習問題に委ねる．

(1) D が $\mathbb{R}$ の斜体である拡大体ならば，それは少なくとも次数 4 である．体の場合のように，すべての元は実数係数の多項式の根である．次数が 3 の場合は $\mathbb{R}$ に根がある．次数が 2 の場合は得られた拡大は可換でなければならない．したがって，$\mathbb{C}$ に同型になる．

(2) D が $\mathbb{R}$ 上次数 4 ならば，それは基底 $1,e_1,e_2,e_3$ をもつ．実数でない基底は $\mathbb{R}$ 上 2 次の多項式を満足しなければならないので，虚数単位と同様な振舞いをするように選ぶことができる．したがって，$e_1^2=e_2^2=e_3^2=-1$ としてよい．D の非可換性によって，$e_1e_2=e_3$ が成り立ち，ゆえに $D\cong H$ を得る．

(3) D が $\mathbb{R}$ 上次数 $n+1$ の多元環であれば，上で説明したような基底 $1,e_1,e_2,\cdots,\ e_n,\ e_i^2=-1(i=1,\ldots,n)$ がある．このとき，任意の対

$i, j\ (i \neq j)$ に対して $e_ie_j + e_je_i \in \mathbb{R}$ となることを示すことができる．これより，e_i を $e_1e'_2 + e'_2e_1 = 0$ を満たす e'_i で置き換えることができる（$e_1e_2 + e_2e_1 = 2c \in \mathbb{R}$ ならば，$e'_2 = (e_2 + ce_1)/\sqrt{1-c^2}$ とすればよい）．このとき，$n > 3$ ならば矛盾にいたることが証明できる ($e_3 = e_1e_2$ としてよい．そのとき，$a_{ij} = e_ie_j + e_je_i$, したがって，$a_{12} = 0$. さらに，$-2e_4 = a_{14}e_1 + a_{24}e_2 + a_{34}e_3$. これは，基底の独立性に矛盾する). ■

以上ここまでで，代数学の基本定理の代数的考察は完了した．この方面からの理解において，基本定理は実数の代数拡大について次のような事柄を言っている．その証明は代数的ではあるけれども，それらは実多項式の連続性，したがって，実数の完備性になお依存している．次の 2 つの章において，位相的に動機づけられた代数学の基本定理の 2 つの証明を検討しよう．

演習問題

7.1　定理 7.1.2 を証明せよ．R が何らかの代数的構造をもてば，Aut(R) は群をつくる．さらに，S がその部分的な構造をもてば，Aut(S) は Aut(R) の部分群である．

7.2　G が位数 6 の巡回群であるとき，Aut(G) の構造を決定せよ．

7.3　G を有限群とし，H をその部分群とする．このとき，$N_G(H)$ は部分群であり，$|G : N_G(H)|$ は G における H の異なる共役の個数に一致することを示せ．

7.4　G をアーベル群とし，H をその部分群とする．このとき，G/H もアーベル群であることを示せ．

7.5　p, q を $p > q$ なる素数とする．G が位数 pq の群ならば，G は正規 p-シロー部分群をもつことを示せ．

7.6　F を有限体とする．F は適当な素数 p が存在して p^n 個の元をもつことを示せ (ヒント：$|F| < \infty$ であるから，char $F \neq 0$ である．ゆえに，その素体は $\mathbb{Z}_p$ と表される．そのとき，F は $\mathbb{Z}_p$ 上のベクトル空間である).

7.7　(a) $\alpha = i + \sqrt{2}$ とするとき，$irr(\alpha, \mathbb{Q})$ と $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ．
(b) $\alpha = \sqrt{3} + \sqrt{7}$ とするとき，$irr(\alpha, \mathbb{Q})$ と $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ を求めよ．

7.8　$\mathbb{Q}(\sqrt{3}+\sqrt{7})=\mathbb{Q}(\sqrt{3},\sqrt{7})$ を示せ（ヒント：次数を計算せよ）．

7.9　$[E:F]=n$ とし，$p(x)\in F[x]$ は F 上で既約であると仮定する．このとき，$\deg p(x)$ と n が互いに素であれば，$p(x)$ は E に根をもたないことを示せ．

7.10　$[E:\mathbb{R}]<\infty$ ならば，$E=\mathbb{R}$ かまたは $E=\mathbb{C}$ であることを示せ．

7.11　$\mathbb{Q}$ 上の多項式 x^3-6 の最小分解体に対して，そのガロア群と部分群の束を決定せよ．

7.12　G を有限群とする．このとき，適当な体 F とそのガロア拡大体 K が存在して，$G=\mathrm{Gal}(K/F)$ が成り立つことを示せ．

7.13　G を群とする．G の元 g_1,g_2 に対して，$g_1g_2g_1^{-1}g_2^{-1}$ なる形の元を**交換子**といい，$[g_1,g_2]$ によって表す．すべての交換子によって生成される G の部分群を交換子部分群といい，G' で表す．

(a) G' は G の正規部分群であることを示せ．

(b) G/G' はアーベル群であることを示せ．

(c) G/H がアーベル群ならば，$G'\subset H$ であることを示せ．

7.14　G を可解群とする．H が G の部分群ならば，H も可解群であることを示せ．さらに，H が G の正規部分群ならば，G/H は可解群であることを示せ．

7.15　H をハミルトンの 4 元数体とし，$\alpha=r_0+r_1i+r_2j+r_3k$ を実 4 元数とする．すなわち，$\alpha\in H$. その共役を $\overline{\alpha}=r_0-r_1i+r_2j+r_3k$ によって定義する．このとき，$\alpha\overline{\alpha}$ は実数であることを示し，これを用いて，0 でない 4 元数の逆元を表せ．

7.16　totally real field F に対して，H_F は多元体をなすことを示せ．

7.17　定理 7.8.3 の完全な証明を与えよ．

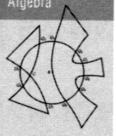
7.18　S_n を n 個の文字の対称群とする．S_n は $\{1,2,\ldots,n\}$ についての置換群と考えることができる．置換 $\sigma\in S_n$ は次の条件を満たすときに，位数 k の**巡回置換**という．$\{1,2,\ldots,n\}$ の適当な部分集合 $\{i_1,i_2,\ldots,i_k\}$ が存在して，$\sigma(i_1)=i_2,\sigma(i_2)=i_3,\ldots,\sigma(i_k)=i_1$ となっている (σ は i_1 から始まって，$\{i_1,i_2,\ldots,i_k\}$ を順番に通って i_1 にもどる)．たとえば，置換 $\begin{pmatrix}3&4&6\\4&6&3\end{pmatrix}$ は S_6 において位数 3 の巡回置換である．巡回置換はその中の任意の整数から始まり，順番にその像を書いていくことによって

表すことができる．3 項巡回置換 $\begin{pmatrix} 3 & 4 & 6 \\ 4 & 6 & 3 \end{pmatrix}$ は (3 4 6) として表される．

(a) S_n のすべての置換は異なった巡回置換の積として表すことができることを示せ（ヒント：$\sigma \in S_n$ と仮定する．1 から始めて，$\sigma(1), \sigma(\sigma(1))$ がどうなるかを追跡する．それは最後に巡回して 1 にもどらねばならない．次に，この巡回置換に現れない最も小さい整数に対して同じことを行う）．たとえば，$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\ 2\ 3)(4\ 5)$.

(b) **互換**は位数 2 の巡回置換である．S_n のすべての置換は互換の積として表すことができる (ヒント：すべての巡回置換は互換の積として表すことができる).

(c) 偶数個の互換の積として表されるの置換の集合は S_n の指数 2 の部分群である．この群は n 個の文字についての**交代群**と呼ばれ，A_n で表される．一般に偶数個の互換の積として表される置換を**偶置換**，そうでないとき**奇置換**という．したがって，交代群は偶置換のつくる部分群であるということができる．



第8章

位相と位相空間

8.1　回転数と代数学の基本定理——証明5

ここまでで，我々は代数学の基本定理について4つの異なった証明を見てきた．はじめの2つは純粋に解析的なものであり，他方，後の2つは広く代数的な概念に関係している．しかしながら，これらの代数的な証明においてさえも，まったく解析学を離れるというわけにはいかなかったということを理解すべきである．代数的な証明のどちらも,「奇数次の多項式は実根をもつ」という事実を用いている．これは中間値の定理から得られる1つの結果であり，中間値の定理は連続性に依存している．連続性は位相的な性質であり，そして，これから位相に関係した概念を用いた代数学の基本定理の2つの証明を考察しよう．

次の曲線を考える．

$$\gamma(t) = z_0 + re^{it},\ 0 \leq t \leq 2n\pi.$$

幾何学的に，これは点 z_0 のまわりを n 回回転している円である．このことをもう少し詳しく見てみよう．積分すると，次のようになる．

$$\frac{1}{2\pi i}\int_\gamma \frac{dz}{z-z_0} = \frac{1}{2\pi i}\int_0^{2n\pi} \frac{r^{it}}{ire^{it}}dt = n.$$

整数 n は点 z_0 のまわりの曲線 γ の**回転数**と呼ばれる．より一般的に，γ を

$\mathbb{C}$ における任意の連続的に微分可能な閉曲線で，$z_0 \in \mathbb{C} - \gamma$ とすれば，

$$n(\gamma, z_0) = \frac{1}{2\pi i}\int_\gamma \frac{dz}{z - z_0}$$

は整数であることが示される．この整数 n は点 z_0 のまわりの曲線 γ の**回転数**と呼ばれる．

さて，関数 $g(z) = z^n$ を考える．C_r を原点を中心とする半径 r の円 $z = re^{it}, 0 \le t \le 2\pi$ とする．この円周上では $z^n = r^n e^{int}$ となっている．t が 0 から 2π まで動けば，z は円周上を 1 回転する．同時に，nt は 0 から $2n\pi$ に動き，したがって，関数 z^n は半径 r^n の円のまわりを n 回回転する．関数 z^n は原点に関して**回転数** n であるという．

この回転数の概念を用いて，代数学の基本定理の第 5 の証明を与える．最初に関数の回転数の概念を一般化しなければならない．γ を連続的に微分可能な閉曲線で，$f : \mathbb{C} \to \mathbb{C}$ を連続関数とすれば，$f(\gamma)$ も閉曲線である．$f(\gamma)$ が z_0 のまわりの回転数 n をもつとき，f は閉曲線 γ を z_0 のまわりに n 回回転するという．我々にとって最も重要であるのは γ が円の場合である．

次に，$f(z)$ と $g(z)$ が原点を中心として半径 r の円 C_r 上で十分近ければ，$f(z)$ と $g(z)$ は原点のまわりで同じ回転数だけ円 C_r を回転する．すなわち，半径 r の円 C_r 上で十分小さな ϵ に対して $|f(z) - g(z)| < \epsilon$ ならば，$f(z)$ と $g(z)$ は原点のまわりで同じ回転数をもつ．

上で説明した事柄はさらに精密にすることができるけれども，ここではただ**同伴者の定理** (fellow-traveler property) と呼ばれる事柄を用いて，それを表現しよう．驚くべきことに，この考えは幾何学的な群論においては非常に重要なものになってきている．1 本のロープによって結ばれた 2 人の旅行者を考えよう．1 人の旅行者 $\{f(z)\}$ が原点の回りの円周上を旅行するとき，ロープの長さ ϵ がその円の半径よりも短ければ，仲間の旅行者 $\{g(z)\}$ も異なった道を通って原点の回りを旅行する．これを図で説明する (図 8.1).

さて，代数学の基本定理の第 5 の証明を与えよう．

定理 8.1.1（代数学の基本定理）任意の定数でない複素多項式は複素数の根をもつ．

（**証明**）$f(z) = a_n z^n + \cdots + a_0$, $a_n \neq 0$, $n \ge 1$ と仮定する．根を求めるた

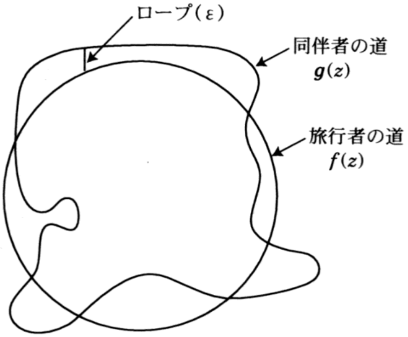


図 8.1　同伴者の定理

めに，$a_n = 1$ と仮定しても一般性を失わないので

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

とする．さらに $a_0 = 0$ ならば，$z = 0$ は根であるから，$a_0 \neq 0$ と仮定してよい．

$f(z)$ は連続関数 $\mathbb{C} \to \mathbb{C}$ であることを思い出そう．さらに，

$$\lim_{z \to \infty} \frac{z^n}{f(z)} = 1$$

であるから，十分大きい円 C_r に対して

$$|z^n - f(z)| \leq \lambda r^n$$

が成り立つ．ただし，$0 < \lambda < 1$ であって，z は C_r 上にある．

任意の $r > 0$ に対して，z^n は原点のまわりの円 C_r を n 回回転している．したがって，同伴者の定理により，$f(z)$ も原点のまわりの十分大きい円 C_r を n 回回転している．

十分小さい円 C_r に対して C_r 上で $f(z) \approxeq a_0$ であるから，$f(C_r)$ は a_0 のまわりに小さな輪をつくり，原点のまわりを回転することはない．$f(z)$ は連続であるから，$f(C_r)$ は r について連続的に依存する．$f(C_r)$ は 小さい半径に対して回転数 0 であり，十分大きい r に対しては原点のまわりを n 回回転するので，$f(C_{r_1})$ が原点を通っているような中間の値 r_1 が存在する．ゆえ

に，$f(z_0) = 0$ を満たす C_{r_1} 上の点 z_0 が存在する．したがって，定理が証明された． ■

次の節において，この証明を代数学の基本定理の一般位相的な証明に拡張する．このために，位相空間論からいくつか基本的な概念と結果を紹介しなければならない．

8.2　位相数学 —— その展望

位相数学は，おもに複素平面のいわゆる位相的性質から発生した数学の大きな一分野の名前である．字義的に位相数学は位置の数学または科学を意味しており，少し前の教科書には，位相数学と同義として使われている**位置解析**という言葉が見いだされる．

複素平面の位相的性質は連続性に関係した性質である．これらの性質は**開集合**，**閉集合**，**コンパクト集合**，そして**連結集合**のような概念を含んでいる．より一般的な連続性の定義をする必要があるが，位相数学は連続な全単射によって保存される性質を扱う．別の言い方をすれば，位相数学は位相空間の研究であって，その位相空間と連続性が定義されることのできる最も一般的な空間として考えられるもののことである．これを第 8.4 節で詳しく論じよう．

歴史的には，位相空間は交差している 2 つの主要な発展の道と研究方法をたどった．これらの最初の道は幾何学から起こった．この方法においては，位相空間は 2 つの形状はお互いに連続的に変形されるときに同値であるとする，一般化された幾何学的な形状として考えられる．このことは位相数学を「ゴムシートの幾何学」へと導いていく．この幾何学においては，2 つの対象は破ることなしにお互いに変形できれば，位相的に同じものであるとみなす．このようにして，円はある意味で位相的に閉曲線と同じものとみなし，円環（空気の入ったチューブ）はハンドルのついた球と同じものとみなす．これらを図 8.2 で示す．

現代の位相数学はゴムシートの幾何学的方法をはるかに越えてしまっている．すなわち，引き裂くこと，切除，貼合せは，それらが連続的なやり方でなされる限り許される．しかしながら，その場合でもゴムシートの幾何学の考え方は一貫しているのである．

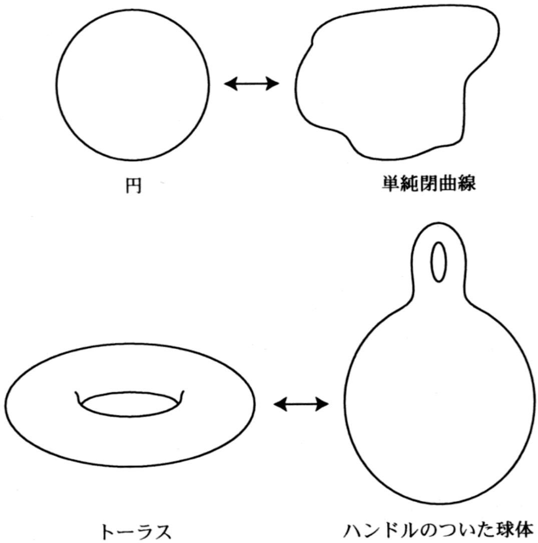


図 8.2　ℂ の部分集合

この幾何学的アプローチにおいては，重要点は空間それ自身の上にある．このアプローチはホモロジー理論とホモトピー理論（次の章で論じる），そして多様体（局所的にユークリッド空間のように見える空間）の位相的理論などへと発展していく．

第 2 の道の位相数学は一般化された解析学のあとをたどる．ここでは，第一の重要点は連続関数とそれらの性質である．それらの空間自身はこれらの関数の単なる定義域と見なされる．このアプローチは一般化されたユークリッド空間——バナッハ空間とヒルベルト空間（これらの空間上で微分と積分の理論が構築される）——などへと発展していく．

位相数学はたくさんの分枝をもち，それらは大きく分けて，2 つのカテゴリーになる．最初のものは**点集合の位相**とよばれるものである．これは直接に位相空間の研究をする．この章で我々が学ぶのはこのアプローチである．第 2 のものは**代数的位相幾何学**と呼ばれるものである．ここでは，位相空間と構造がそれらに付随した代数的対象（群と環）の言葉によって研究される．このアプローチは代数学の基本定理の最後の証明に我々を導いていく．これは次の章で見ていく．

8.3 連続性と距離空間

前節において述べたように，位相数学とその特質は連続性の概念から発生した．ここでは，はじめにこの概念を復習し，それから発展させよう．

1 変数の実数値関数 $y = f(x)$ は次の条件を満たすとき，点 x_0 で**連続**であるという．任意の $\epsilon > 0$ に対して，ある実数 $\delta > 0$ (ϵ と x_0 に依存する) が存在して，$0 \leq |x - x_0| < \delta$ ならば $|f(x) - f(x_0)| < \epsilon$ である．区間 $[a, b]$ の各点において連続であるとき，関数 $y = f(x)$ は $[a, b]$ で連続であるという．この定義においては，絶対値は実直線上の距離を測るために用いられていることに注意しよう．したがって，この定義は次のように言いかえることができる．任意の ϵ に対して，ある実数 δ が存在して，x と x_0 の距離が δ より小さければ，$f(x)$ と $f(x_0)$ の距離も ϵ より小さい．

第 4 章で複素数に対して見たように，この定義を $\mathbb{R}^2$ 上で定義された実数値関数にほとんど逐次的に拡張することができる．すなわち，$P_0 = (x_0, y_0)$ とおく．実数値関数 $z = f(x, y)$ は次の条件を満たすとき，点 P_0 で連続であるという．任意の $\epsilon > 0$ に対して，ある実数 $\delta > 0$ (再び ϵ と P_0 に依存する) が存在して，$|(x, y) - (x_0, y_0)| < \delta$ ならば $|f(x, y) - f(x_0, y_0)| < \epsilon$ である．上記における絶対値は $\mathbb{R}^2$ における距離の意味である．距離の言葉でこれを言い換えてみよう．この言換えは問題になっている概念を拡張するための離陸点としての機能を果たす．まず最初に，実直線 $\mathbb{R}$ または平面 $\mathbb{R}^2$ において，$d(x, y)$ を点 x, y の間の距離と呼ぶことにしよう．このとき，$\mathbb{R}^2$ から $\mathbb{R}$ への関数 $z = f(P)$ は次の条件を満たすとき，点 $P_0 \in \mathbb{R}^2$ で連続であるという．任意の ϵ に対して，ある実数 $\delta > 0$ が存在して，$d(P, P_0) < \delta$ ならば $d(f(P), (f(P_0)) < \epsilon$ である (はじめの d は $\mathbb{R}$ における距離で，後のほうの d は $\mathbb{R}^2$ における距離であることに注意しよう)．さらに，1 変数関数 $z = f(P)$ について，$\mathbb{R}^2$ におけるある集合上の任意の点において連続であるとき，$z = f(P)$ はその集合上で連続であるという．$\mathbb{R}$ と $\mathbb{R}^2$ における連続性の定義は，距離が定義されれば，任意の実 n 次元空間 $\mathbb{R}^n$ に拡張することができる．

定義 8.3.1 $P_1 = (x_1, \ldots, x_n), P_2 = (y_1, \ldots, y_n)$ とする．このとき，P_1 から

P_2 への距離は，$d(P_1, P_2)$ によって表され，次の式によって定義される．

$$d(P_1, P_2) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}.$$

これは $\mathbb{R}^2$ における距離の公式の単なる一般化であることに注意しよう．この距離の定義は通常距離に付随している基本的な性質をすべて満足している．このことを確かめることは容易である（演習問題参照）．

補題 8.3.1　$d : \mathbb{R}^n \to \mathbb{R}$ を上で定義された $\mathbb{R}^n$ 上の距離関数とする．このとき，次が成り立つ．

(1) $d(P_1, P_2) \geq 0$ がすべての $P_1, P_2 \in \mathbb{R}^n$ に対して成り立つ．また，$d(P_1, P_2) = 0$ であるのは $P_1 = P_2$ のときに限る．

(2) $d(P_1, P_2) = d(P_2, P_1)$ がすべての $P_1, P_2 \in \mathbb{R}^n$ に対して成り立つ．

(3) $d(P_1, P_2) \leq d(P_1, P_3) + d(P_3, P_2)$（三角不等式）がすべての $P_1, P_2, P_3 \in \mathbb{R}^n$ に対して成り立つ．

距離関数を定義したので，連続性を定義することができる．このとき，連続関数の値域は $\mathbb{R}$ に限る必要はない．

定義 8.3.2　$f : \mathbb{R}^n \to \mathbb{R}^m$ とする．f は次の条件を満たすとき，$P_0 \in \mathbb{R}^n$ で**連続**であるという．任意の ϵ に対して，ある実数 $\delta > 0$ が存在して，$d(P, P_0) < \delta$ ならば $d(f(P), (f(P_0)) < \epsilon$ である．関数 f は集合 $U \subset \mathbb{R}^n$ の任意の点で連続であるとき，集合 U 上で**連続**であるという．

上のすべての議論において，連続性を定義するためにただ 1 つ必要なことは，距離を測ることができることである．このことを抽象化して，距離を測ることのできる一般的な空間を考察する．

定義 8.3.3　M を空でない集合とする．M 上の**距離**あるいは，**距離関数**とは，次の条件を満たす関数 $d : M \times M \to \mathbb{R}$ のことである．

(1) $d(x, y) \geq 0$ がすべての $x, y \in M$ に対して成り立つ．また，$d(x, y) = 0$ であるのは $x = y$ のときに限る．

(2) $d(x,y)=d(y,x)$ がすべての $x,y\in M$ に対して成り立つ.

(3) $d(x,y)\leq d(x,z)+d(z,y)$ がすべての $x,y,z\in M$ に対して成り立つ (これは**三角不等式**と呼ばれる).

距離空間とは，集合 M とその上で定義されている距離 d からなる対 (M,d) のことである.

例 8.3.1

(1) 任意の $n\geq 1$ に対して，n 次元実空間 $\mathbb{R}^n$ は定義 8.3.1 で定義された距離をもつ距離空間である．この距離をもつ $\mathbb{R}^n$ は **n 次元ユークリッド空間**と呼ばれる.

(2) $C^0[a,b]$ を閉区間 $[a,b]$ で定義されたすべての連続関数からなる集合とする．$f(x),g(x)\in C^0[a,b]$ に対して，次のように定義する.

$$d(f(x),g(x))=\left(\int_a^b|f(x)-g(x)|^2dx\right)^{1/2}.$$

これによって，$C^0[a,b]$ 上に 1 つの距離が定義され，この距離をもつ $C^0[a,b]$ は距離空間となる.

(3) $C^0[a,b]$ を閉区間 $[a,b]$ で定義されたすべての連続関数からなる集合とする．$f(x),g(x)\in C^0[a,b]$ に対して，今度は次のように定義する.

$$d(f(x),g(x))=\max_{x\in[a,b]}|f(x)-g(x)|.$$

これによっても，$C^0[a,b]$ 上に 1 つの距離が定義され，$C^0[a,b]$ はこの距離をもつ（異なった）距離空間となる.

この最後の 2 つの例は，1 つの集合はその上に 1 つ以上の距離をもつことが可能であることを示している．特に，任意の集合 M は $x=y$ のとき $d(x,y)=0$, $x\neq y$ のとき $d(x,y)=1$ と定義することによって距離空間にすることができる．しかし，多くの場合これはあまり興味をひくものではない.

□

例 8.3.1 (2),(3) における距離空間は実ベクトル空間のある類型から発生する一般的距離空間の特別なものである．これらは解析学においては重要な役割をしているので，ここで簡単に紹介しよう.

定義 8.3.4 V を実数 $\mathbb{R}$ 上のベクトル空間とする．このとき，V 上の**内積**とは，次の条件を満たす関数 $\langle\ \rangle : V \times V \to \mathbb{R}$ のことである．

(1) $\langle x, x\rangle \geq 0$ が任意の $x \in V$ に対して成り立つ．$\langle x, x\rangle = 0$ となるのは $x = 0$（ゼロベクトル）のときに限る．

(2) $\langle x, y\rangle = \langle y, x\rangle$ が任意の $x, y \in V$ に対して成り立つ．

(3) $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$ が任意の $x, y, z \in V$ に対して成り立つ．

(4) $\langle \alpha x, y\rangle = \alpha\langle x, y\rangle$ が任意の $x, y \in V$ と $\alpha \in \mathbb{R}$ に対して成り立つ．

内積空間とは，その上に内積の定義されたベクトル空間 V のことである．

V 上の**ノルム**とは，次の条件を満たす関数 $|\,| : V \to \mathbb{R}$ である．

(1) $|x| \geq 0$ が任意の $x \in V$ に対して成り立つ．$|x| = 0$ となるのは $x = 0$ のときに限る．

(2) $|\alpha x| = |\alpha||x|$ が任意の $x \in V, \alpha \in \mathbb{R}$ に対して成り立つ．

(3) $|x + y| \leq |x| + |y|$ $(x, y \in V)$ が任意の $x, y \in V$ に対して成り立つ．

ノルム空間とは，その上にノルムが定義されたベクトル空間 V のことである．

例 8.3.2 $P_1 = (x_1, \ldots, x_n), P_2 = (y_1, \ldots, y_n) \in \mathbb{R}^n$ に対して，内積を

$$\langle P_1, P_2\rangle = \sum_{i=1}^{n} x_i y_i$$

と定義すれば，$\mathbb{R}^n$ は内積空間である．さらに，$\mathbb{R}^n$ は $|P_1| = \sqrt{\sum_{i=1}^{n} x_i^2}$ によってノルム空間になっている．

これらが実際に内積であること，および $\mathbb{R}^n$ 上のノルムであることを確かめるのは容易である．しかしながら，$\mathbb{R}^n$ は一種の包括的な例としての役目を果たす．また，$P_1, P_2 \in \mathbb{R}^n$ ならば，上で定義されたノルムに対して $d(P_1, P_2) = |P_1 - P_2|$ が成り立つ．□

これらのベクトル空間は次の補題によって，我々の議論に関連のあるものとなる．

補題 8.3.2 任意の内積空間 V は $d(x, y) = |x - y|$ $(x, y \in V)$ によって距離空間になる．

（証明）$d(x,y)=|x-y|$ と定義する．$d(x,y)\geq 0$ であることと，$d(x,y)=0$ であるための必要十分条件は $x=y$ であることはノルムの性質 (1) から直接得られる．同様に，$d(x,y)=|x-y|=|-1||y-x|=d(y,x)$. 最後に，$d(x,y)=|x-y|=|x-z+z-y|\leq|x-z|+|y-z|=d(x,z)+d(y,z)$. ■

補題 8.3.3 V を内積空間とする．任意の $v\in V$ に対して，$|v|=\sqrt{\langle v,v\rangle}$ と定義する．そのとき，これは V 上にノルムを定義する．特に，任意の内積空間はノルム空間になり，さらに，距離空間となる．

（証明）補題 8.3.2 の証明のように，ノルムの性質を示すために内積の性質を使う．$|v|=\sqrt{\langle v,v\rangle}$ より，$|v|\geq 0$ ($\langle v,v\rangle\geq 0$ だから). また，$|v|=0\Leftrightarrow v=0$.

さらに，$|\alpha v|=\sqrt{\langle\alpha v,v\alpha\rangle}=\sqrt{\alpha^2\langle v,v\rangle}=|\alpha||v|$.

最後の性質を示すために，次の重要な結果を必要とする．この結果は任意の内積空間で成り立ち，その証明は演習問題にゆだねる． ■

コーシー・シュワルツの不等式

任意の内積空間 V の任意の元 $u,v\in V$ に対して，次が成り立つ．

$$|\langle u,v\rangle|\geq|u||v|.$$

この定理を使えば，

$$\begin{aligned}|u+v|^2 &= \langle u+v,u+v\rangle=\langle u,u\rangle+2\langle u,v\rangle+\langle v,v\rangle\\ &\leq \langle u,u\rangle+2|\langle u,v\rangle|+\langle v,v\rangle\\ &\leq |u|^2+2|u||v|+|v|^2=(|u|+|v|)^2.\end{aligned}$$

平方根をとれば，次の式を得る．

$$|u+v|\leq|u|+|v|.$$

これで，前の補題の証明が完結した．

$\mathbb{R}^n$ と例 8.3.1 において導入した空間は 2 つとも内積空間である．

定理 8.3.1 $C^0[a,b]$ を閉区間 $[a,b]$ の上で連続なすべての関数の集合とする．任意の $f(x),g(x)\in C^0[a,b]$ に対して，

$$\langle f,g\rangle=\int_a^b f(x)g(x)dx$$

と定義する．そのとき，$C^0[a,b]$ は内積空間となり，ゆえにノルム空間である．したがって，それは距離空間となる．

(証明) 連続関数の加法，減法，そして実数のスカラー乗法は連続性を保存する．したがって，$C^0[a,b]$ は実ベクトル空間になる．これが内積空間であることを示すために，内積の性質を示さなければならない．

(1) $\langle f,f\rangle = \int_a^b (f(x))^2dx \geq 0$. $\langle f,f\rangle = 0$ ならば，$\int_a^b (f(x))^2dx = 0$. $f(x)$ は連続関数であるから，これは $f(x) \equiv 0$ を意味している．

(2) $\langle f,g\rangle = \int_a^b f(x)g(x)dx = \int_a^b g(x)f(x)dx = \langle g,f\rangle$.

(3) $\langle \alpha f,g\rangle = \int_a^b \alpha f(x)g(x)dx = \alpha \int_a^b g(x)f(x)dx = \alpha\langle g,f\rangle$.

(4) $\langle f+g,h\rangle = \int_a^b (f(x)+g(x))h(x)dx = \int_a^b f(x)h(x)dx = \int_a^b g(x)h(x)dx = \langle f,h\rangle + \langle g,h\rangle$. ■

さて，ここで我々の主要な議論にもどろう．連続性は距離にのみ依存するので，任意の距離空間において定義することができる．

定義 8.3.5 $(M_1,d_1),(M_2,d_2)$ を距離空間とする．関数 $f : M_1 \to M_2$ は次の条件を満たすとき，$x_0 \in M_1$ で**連続**であるという．任意の $\epsilon > 0$ に対して，ある実数 $\delta > 0$ が存在して，$d(x,x_0) < \delta$ ならば $d(f(x),(f(x_0)) < \epsilon$ である．関数 f は M_1 の任意の点で連続であるとき，M_1 上で**連続**であるという．

これらの考えをより一般的な位相空間に拡張するために，距離関数に依存することを止めなければならない．このために，他の考えを導入する．

定義 8.3.6 (M,d) を距離空間とする．$x_0 \in M$ に対して，x_0 を中心とする半径 $\epsilon > 0$ の**開球体** $S_\epsilon(x_0)$ を次のように定義する．

$$S_\epsilon(x_0) = \{x \in M \,:\, d(x,x_0) < \epsilon\}.$$

集合 $S \subset M$ は，すべての点 $x_0 \in S$ に対して，S に完全に含まれている x_0 を中心とする開球体が存在するとき，**開集合**という．集合 $C \subset M$ は，その補集合 C' が開集合であるとき**閉集合**という．

これらの定義は第 4 章で論じたように，複素平面における開集合と閉集合の概念を一般化したものであることに注意しよう．

定理 8.3.2 (M, d) を距離空間とする．このとき，次が成り立つ．

(1) 開集合の任意の和集合は開集合である．

(2) 有限個の開集合の共通集合は開集合である．

この定理は次のように簡潔に表現される．すなわち，任意の距離空間において，開集合の族は任意の和集合をとる操作と有限個の共通集合をとる操作において閉じている．

この考えを連続性の定義から距離関数を除くために用いる．はじめに，S が開集合で $x \in S$ とするとき，S は x の**開近傍**という．次の補題は開球体の言葉を使って，連続性の定義を言い換えたものである．

補題 8.3.4 関数 $f : M_1 \to M_2$ は次の条件を満たすとき，$x_0 \in M_1$ で連続である．$f(x_0)$ を中心とする任意の開球体 $S_\epsilon(f(x_0))$ に対して，ある開球体 $S_\delta(x_0)$ が存在して，$f(S_\delta(x_0)) \subset S_\epsilon(f(x_0))$ となっている．言い換えると，$f(x_0)$ の任意の開近傍 S に対して，その逆像 $f^{-1}(S)$ が x_0 の開近傍であるとき f は x_0 で連続である．

上の補題の後半を拡張すると次のようになる．

補題 8.3.5 関数 $f : M_1 \to M_2$ は，任意の開集合 $O \subset M_2$ に対して，$f^{-1}(O)$ が M_1 において開集合であるとき，M_1 上で連続である．

次の節において，連続性の定義として補題 8.3.5 を採用する．その前に，読者が解析学においてなじみのある他のいくつかの考えについて見てみよう．これらのものは，代数学の基本定理の我々の最後の証明においては使われないが，上の議論と深く結びついている．

閉集合を開集合の補集合として定義した．ほとんどの人ははじめに，閉集合をそれらの境界を含んでいる集合として出会う．これらの概念は，すぐ後に述べる次の概念によって同じものと考えられるようになる．

定義 8.3.7 (M,d) を距離空間とし，(x_n) を M における点列とする．任意の $\epsilon > 0$ に対して，ある自然数 N が存在して，すべての $n \geq N$ に対して $x_n \in S_\epsilon(x_0)$ となるとき，$x_n \to x_0$ と書く．$S \subset M$ とする．このとき，$x \in M$ は適当な S の列 (x_n) が存在して $x_n \to x_0$ であるとき，S の**極限点**という．点 $x_0 \in S$ は適当な $\epsilon > 0$ が存在して $S_\epsilon(x_0) \subset S$ となるとき，S の **内点**という．S の**境界**とは，S の内点でないすべての極限点の集合のことである．

定理 8.3.3 (M,d) を距離空間とする．このとき，$C \subset M$ が閉集合であるための必要十分条件は，C がそのすべての極限点を含んでいることである．

最後に，連続性の定義において，δ という数は与えられた ϵ と特別な点 x_0 に依存していた．距離空間においては連続性よりさらに強い概念を定義することができる．

定義 8.3.8 関数 $f: M_1 \to M_2$ は次の条件を満たすとき，M_1 で**一様連続**であるという．すなわち，任意の ϵ に対して，ある実数 $\delta > 0$ が存在して (これは ϵ にのみ依存する)，$d(x_1, x_2) < \delta$ ならば $d(f(x_1), (f(x_2)) < \epsilon$ となる．

一様連続ならば明らかに連続である．$\mathbb{R}^n$ において，逆は十分良い領域上で真である．すなわち，次の定理が成り立つ．

定理 8.3.4 $f: \mathbb{R}^n \to \mathbb{R}^m$ は $M \subset \mathbb{R}^n$ で連続とする．M が閉集合で有界（コンパクト）ならば，f は M 上で一様連続である．

一様連続性は実際距離的な性質である．次の節においてそうするように，距離という概念を放棄すると，本質的に一様連続性の概念も失うことになる．

8.4　位相空間と同相写像

前節において 1 つの距離空間から別の距離空間への連続写像の概念を議論した．この定義は各空間上の距離の言葉で定式化され，しかしその後で開集合の言葉で再び定式化した．ここで我々がしようと思っていることは，距離を用いないで連続性を定義することである．そのために，開集合の集まりを考えなければならず，それは我々を位相空間の概念へと導くことになる．

定義 8.4.1. X を空でない集合とする．X 上の**位相**とは次の条件を満たす部分集合の族 T である．

(1) 空集合 $\emptyset$ と全体集合 X は T に属している．

(2) T における部分集合の任意の族の和集合は T に属する．

(3) T における部分集合の有限個の族の共通集合は T に属する．

このように，1 つの位相とは，任意の和集合と有限個の共通集合をとる操作において閉じている部分集合の族である．T に属している部分集合は**開集合**と呼ばれ，一方開集合の補集合は**閉集合**と呼ばれる．

位相空間とは，その上で定義された位相をもつ集合 X のことである．X の元は**点**と呼ばれ，その位相は X の**開集合**の族と呼ばれる．

任意の距離空間において，開集合の族は，任意の和集合をとる操作と有限個の共通集合をとる操作において閉じているので，1 つの位相を構成する．

補題 8.4.1. 任意の距離空間は位相空間である．特に，$\mathbb{R}^n$ とより一般的な任意の内積空間は位相空間である．

すべての位相空間が距離空間であるとは限らない．いくつか他の例をあげよう．

例 8.4.1. X を空でない集合とし，T を X のすべての部分集合とする．このとき，T は**離散位相**と呼ばれる X 上の位相を定義する． □

例 8.4.2. X を空でない集合とし，$T = \{\emptyset, X\}$ とする．このとき，T は X 上の位相である． □

例 8.4.3. X を無限集合とする．T を空集合と，その補集合が有限集合であるすべての部分集合から構成されているとする．そのとき，T は 1 つの位相をつくる（演習問題参照）．この位相を X 上の **cofinite topology** という． □

たくさんの様々な位相空間の例が与えられたとき，当然起こってくるのは，どれが実際距離空間であるかという問題である．一般位相空間 X は，その開

集合が与えられた位相における開集合と一致しているような X 上の距離が少なくとも 1 つ存在しているとき，**距離づけ可能**であるという．次の節において，距離づけ可能であるための十分条件を与える．

さて，連続性の概念を拡張しよう．

定義 8.4.2. X, Y を位相空間とし，$f : X \to Y$ とする．Y の任意の開集合 O に対して，$f^{-1}(O)$ が X において開集合であるとき，f は**連続関数**，または**連続写像**という．したがって，連続関数は開集合を開集合に引き戻す．

関数 $f : X \to Y$ は，X の任意の開集合 V に対して，$f(V)$ が Y において開集合であるとき，**開写像**という．したがって，開写像は開集合を開集合に移す．

定義 8.4.3. 2 つの位相空間 X, Y の間の**同相写像**とは，X から Y の上への 1 対 1 の連続写像でかつ開写像となっているものである．この写像は連続な全単射で，その逆写像も連続であるものとして定義することもできる．

同相写像 $f : X \to Y$ が存在するとき，X, Y は**同相空間**であるという．

同相写像は，代数学において同型写像が果たした役割を位相数学において果たす．すなわち，同相空間は本質的に「位相的に同じもの」である．位相数学における**分類問題**は同相写像を除いて位相空間を分類（区別）することである．

8.5　位相空間

代数的位相と代数学の基本定理の我々の最後の証明に移るまえに，点集合の位相からさらにいくつかの結果と性質に言及しよう．特に，4 つの性質，**分離性**，**距離づけ可能性**，**コンパクト性**，そして**連結性**を考察する．これらはすべてユークリッド空間 $\mathbb{R}^n$ においてそれらに対応するものに動機づけられている．

任意の距離空間は次の分離的な性質をもっている．異なった 2 点を $x, y \in M$ とするとき，$x \in O_1, y \in O_2$ を満たす共通部分のない開集合 O_1, O_2 が存在する．これは図 8.3 より明らかである．このためには，x と y の開球でそれら

の半径の和が x と y の距離よりも小さい (x と y は異なっているから，それらの距離は 0 ではない) ものをとればよい．

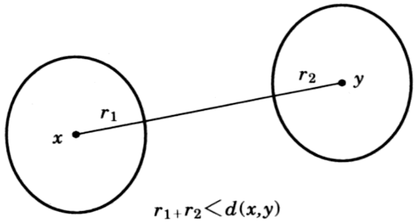


図 8.3 分離的

このことから，距離空間における任意の点はそれ自身閉集合であることがわかる．少し考えれば（演習問題参照），これを次の性質に拡張することができる．M を距離空間とし，F_1, F_2 を M の 2 つの共通部分のない閉集合とするとき，$F_1 \subset O_1, F_2 \subset O_2$ を満たす 2 つの共通部分のない開集合 O_1, O_2 が存在する．次に，これらの考えを位相空間に一般化し，このことより，距離づけ可能性を保証するための十分条件を与えることができる．

定義 8.5.1

(1) 位相空間 X はその任意の点が閉集合であるとき，**T_1-空間**と呼ばれる．

(2) 位相空間 X は, X の異なる点 x, y に対して，$x \in O_x, y \in O_y$ を満たす共通部分のない開集合 O_x, O_y が存在するとき，**ハウスドルフ空間**と呼ばれる．

(3) 位相空間 X は, T_1-空間であって，さらに次の性質を満たすとき，**完全正則空間** (あるいは T_3-空間) と呼ばれる．与えられた閉集合 F と $x \notin F$ なる点に対して，ある連続関数 $f: X \to [0,1]$ が存在して $f(x) = 0$ で $f \equiv 1$(F 上で) を満たす．

(4) 位相空間 X は, T_1-空間であって，さらに次の性質を満たすとき，**正規空間** (あるいは T_4-空間) と呼ばれる．X の与えられた共通部分のない閉集合 F_1 と F_2 に対して，$F_1 \subset O_1, F_2 \subset O_2$ を満たす 2 つの共通部分のない開集合 O_1, O_2 が存在する．

定理 8.5.1 位相空間において，正規空間ならば完全正則空間，完全正則空間ならばハウスドルフ空間, ハウスドルフ空間ならば T_1 空間である．

上の定理において，完全正則空間から後の証明は容易である．正規空間ならば完全正則空間であるという事実は，ウリゾーンの補題と呼ばれる結果の帰結である（演習問題参照）．さらに，上の議論より，任意の距離空間は正規空間であり，したがって，完全正則空間でかつハウスドルフ空間であることがわかる．

分離公理を用いれば，距離づけ可能性を保証する判定基準を与えることができる．前節より次の定義を思い出そう．位相空間は，その位相が X 上に与えられた位相と一致する X 上の少なくとも 1 つの距離が存在すれば，**距離づけ可能**である．

定義 8.5.2　X を位相空間とする．X に対する**開基底**とは開集合の族 B で，任意の開集合は B に属する集合の和集合として表されるようなもののことである．可算個の開基底をもつ位相空間を**第 2 可算空間**という．

正規性をもつ第 2 可算空間は距離付け可能性を保証するのに十分である．

定理 8.5.2（ウリゾーンの埋蔵定理）X が第 2 可算空間でありかつ正規空間ならば，X は距離づけ可能である．

定理 8.5.2 の証明はその空間を距離空間 $\mathbb{R}^\infty$ に埋め込むことに基づいている（したがって，埋蔵定理と呼ばれている）．この距離空間は $\sum_{i=1}^{\infty}|x_i|^2$ が収束するようなすべての実数列 $\{x_1,\ldots,x_n,\ldots\}$ からなる空間である．この空間上で，距離は次のように定義する．$x=\{x_1,\ldots,x_n,\ldots\}, y=\{y_1,\ldots,y_n,\ldots\}$ とするとき，$d(x,y)=(\sum_{i=1}^{\infty}|x_i-y_i|^2)^{1/2}$. これは明らかに，有限の n に対する $\mathbb{R}^n$ 上の距離の一般化である．ある空間が距離空間に埋め込み可能であれば，それはそれ自身距離空間である．

我々が考察する 3 番目の性質は**コンパクト性**である．$\mathbb{R}^2$ におけるハイネ・ボレルの定理によれば，C が $\mathbb{R}^2$ の有界閉集合ならば，開集合による C の任意の被覆は有限個の部分被覆をもつ．この定理の 1 つの帰結として，有界閉集合上の連続な実数値関数は一様連続であるという命題が得られる．ハイネ・ボレルの定理と一様連続性についての命題は任意の有限次元実空間 $\mathbb{R}^n$ に拡張することができる．この性質の位相空間における一般化は**コンパクト**と呼ばれる．位相空間 X において，開集合の族 $\{O_i\}$ が $X\subset\bigcup_i O_i$ を満たすと

き，X の**開被覆**という．X の開被覆の部分族でかつ X を被覆しているものを**部分被覆**という．

定義 8.5.3 位相空間 X は，あるいはより一般的に X のある部分集合は，すべての開被覆が有限な部分被覆をもつとき，**コンパクト**であるという．

ハイネ・ボレルの定理は次のように言い換えることができる．

定理 8.5.3 （ハイネ・ボレル）$\mathbb{R}^n$ の部分集合がコンパクトであるための必要十分条件は，その集合が有界閉集合なることである．

コンパクト空間は位相数学において重要な役割を果たす．ここでは，その非常に良い性質を 2 つあげておこう．

定理 8.5.4 任意のコンパクトハウスドルフ空間は正規空間である．

定理 8.5.5 X をコンパクト空間とし，$f: X \to Y$ を連続関数とする．このとき，f による X の像は Y でコンパクトである．

$\mathbb{R}^n$ の部分集合がコンパクトであるための必要十分条件は，その集合が有界閉集合なることであるから，上の結果はコンパクト集合上の任意の実数値連続関数は有界であることを意味している．特に，$f(z)$ が連続な複素関数ならば，原点のまわりの任意の閉球体上でその値 $|f(z)|$ は有界である．

最後に見る性質は**連結性**である．直感的に，連結な位相空間は一つながりのものである．この性質は中間値の定理に密接に結びついており，それは代数学の基本定理の我々の証明において大きな役割を果たしてきた．

定義 8.5.4 位相空間 X, あるいはより一般的に X の部分集合 Y は，次の性質をもつとき**連結**であるという．O_1, O_2 が開集合で $X = O_1 \cup O_2$, $O_1 \cap O_2 = \emptyset$ ならば，O_1 と O_2 のどちらかは空集合である．すなわち，X は共通部分のないどんな 2 つの開集合（空集合でない）の和集合としても表すことができないときに連結である．共通部分のない 2 つの開集合（空集合でない）の和集合に分解することが可能ならば，X は**非連結**であると呼ばれる．

中間値の定理への結びつきは次のようである．

定理 8.5.6 任意の部分集合 $Y \subset \mathbb{R}$ が連結であるための必要十分条件は Y が 1 つの区間になることである．

定理 8.5.7 X が連結で $f: X \to Y$ が連続ならば，$f(X)$ は連結である．

系 8.5.1 $f: \mathbb{R} \to \mathbb{R}$ が連続ならば，1 つの区間の像は 1 つの区間である．

系 8.5.1 は完全に中間値の定理に同値であり，一般化することができる．

系 8.5.2 $f: D \to \mathbb{R}$ を連続であるとする．ただし，D は $\mathbb{R}^n$ の連結な集合とする．このとき，f は f の値の中の任意の 2 つの値の間の任意の値をとる．

演習問題

8.1　補題 8.3.1 を証明せよ．すなわち，$\mathbb{R}^n$ における距離はすべての基本的な距離の性質を満たす．

8.2　$C^0[a,b]$ を閉区間 $[a,b]$ 上のすべての連続関数の集合とする，$f(x), g(x) \in C^0[a,b]$ に対して，

$$d(f(x), g(x)) = \left(\int_a^b |f(x) - g(x)|^2 dx \right)^{1/2}$$

と定義する．このとき，これは $C^0[a,b]$ 上に 1 つの距離を定義し (例 8.3.1)，この距離によって，$C^0[a,b]$ は距離空間になることを証明せよ．

8.3　$C^0[a,b]$ を閉区間 $[a,b]$ 上のすべての連続関数の集合とする．$f(x), g(x) \in C^0[a,b]$ に対して，

$$d(f(x), g(x)) = \max_{x \in [a,b]} |f(x) - g(x)|$$

と定義する．このとき，これは $C^0[a,b]$ 上に 1 つの距離を定義し，この距離によって，$C^0[a,b]$ は再び（異なった）距離空間になることを証明せよ．

8.4　n 次元実ベクトル空間は内積空間になることを示せ．ただし，$P_1 = (x_1, \ldots, x_n), P_2 = (y_1, \ldots, y_n)$ に対して次のように定義する．

$$\langle P_1, P_2 \rangle = \sum_{i=1}^{n} x_i y_i.$$

8.5　コーシー・シュワルツの不等式を証明せよ．すなわち，V を任意の内積空間とするとき，任意の $u, v \in V$ に対して次が成り立つ．

$$\langle u, v \rangle \leq |u||v|$$

(ヒント：$t \in \mathbb{R}$ に対して，$\langle u - tv, u - tv \rangle$ を考えよ，そのとき，$t = \langle u, v \rangle / \langle v, v \rangle$ とせよ)．

8.6　定理 8.3.2 を証明せよ．すなわち，距離空間 (M, d) において，次を示せ．
(1) 開集合の任意の和集合は開集合である．
(2) 有限個の任意の開集合の共通集合は開集合である．

8.7　(M, d) を距離空間とする．このとき，$C \subset M$ が閉集合であるための必要十分条件は，C がすべての極限点を含んでいることである (定理 8.3.3)．

8.8　X を無限集合とする．T を空集合と，その補集合が有限集合であるすべての X の部分集合とする．このとき，T は X に位相を定義することを示せ (例 8.4.3)．T は X 上の **cofinite topology** と呼ばれる．

8.9　距離空間 M と M の 2 つの共通部分のない閉集合 F_1, F_2 が与えられたとき，$F_1 \subset O_1, F_2 \subset O_2$ を満たす開集合 O_1, O_2 が存在することを示せ (ヒント：M において，F が閉集合で，$x \in F$ ならば，ある数 $\epsilon > 0$ が存在して，すべての y に対して $d(x, y) > \epsilon$ が成り立つ)．

8.10　任意の位相空間において，完全正則空間ならばハウスドルフ空間であり，そして，ハウスドルフ空間ならば T_1 空間であることを示せ．

8.11　ウリゾーンの補題は次のように述べられる．任意の正規空間 X において，与えられた共通部分のない閉集合 A, B に対して，$f(A) \equiv 0, f(B) \equiv 1$ を満たす連続関数 $f : X \to [0, 1]$ が存在する．これを用いて，正規空間ならば完全正則空間であることを証明せよ．

8.12　ハウスドルフ空間において，点 x と x を含んでいないコンパクト集合 F が与えられたとき，それらは共通部分をもたない開集合によって分離されることを証明せよ (ヒント：各 $f \in F$ 点に対して，共通部分をもた

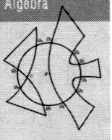
ない開集合 $x \in O_x, f \in O_f$ を考える．このとき，F は O_x の和集合に含まれる．それから，コンパクト性を使えばよい).

8.13 ハウスドルフ空間のコンパクト部分空間は閉集合であることを証明せよ（ヒント：前問を使う）.

8.14 $\mathbb{R}$ の部分集合が連結であるための必要十分条件はそれが区間になることである．これを証明せよ．

8.15 連続関数による，$\mathbb{R}$ の区間の像が再び区間になるという事実は中間値の定理と同値であることを示せ．

8.16 連続写像によるコンパクト集合の像はコンパクトであることを証明せよ (定理 8.5).



第9章

代数的位相幾何学と最後の証明

9.1 代数的位相幾何学

前章において，多項式の回転数を考察することによって，代数学の基本定理の第 5 の証明を与えた．このことは，我々を位相と位相空間の議論へと導いた．さて，この最後のものを模範としたより一般的な証明を呈示しよう．このために，**代数的位相幾何学**の基本的な概念と技術のいくつかを導入し，発展させなければならない．

位相空間 X と Y は，全単射 $f: X \to Y$ が存在して，f と f^{-1} が連続になっているとき，同相であるということを思い出そう．位相数学における主要な問題は，同相を除いて位相空間を分類することである．**代数的位相幾何学**とは，位相空間に代数的対象，主に群を付随させることによってこの分類問題を解こうとする位相数学の分野である．この付随のさせ方は，同相空間は同型な代数的対象に対応しているというような方法でなされる．そのとき，対応している代数的対象が同型でないことが示されれば，その関係している位相空間は同相ではない．代数的な問題は通常対応している位相的な問題よりも簡単であるから，この代数的な環境に変換することによって，分類問題は幾分単純になる．

代数的位相幾何学は**代数的位相不変量**を見いだす問題を扱う．**位相不変量**とは同位相写像によって不変であるであるような，位相空間に付随したもの（対象，数，属性）である．したがって，代数的位相不変量とは，同相写像によっ

て不変な位相空間に付随した代数的対象である．

位相空間に付随した群を見いだすために一般的な 2 つの方法，**ホモトピー理論**と**ホモロジー理論**がある．はじめに，ホモトピー理論を論じよう．

X, Y を位相空間，$f : X \to Y, g : X \to Y$ を連続写像とする．このとき，大まかに言うと，f が連続的に g に変形できるとき，f は g に**ホモトープ**であるという．これは，第 9.3 節において正確に論じようとしている概念である．空間 X, Y は，連続写像 $f : X \to Y, g : Y \to X$ が存在して $f \circ g$ が Y 上の恒等写像にホモトープであり，$g \circ f$ が X 上の恒等写像にホモトープであるとき，**ホモトープ**である，または**ホモトープ同値**であるという．直観的には，ホモトピーは次のように幾何学的に図示することができる．X は連続的に変形することができ，そのとき縮めたり，伸ばしたり，あるいは摘んだりして Y にすることができるとき，X は Y にホモトープである．X, Y が同相であれば，それらはホモトープである．しかしながら，空間は同相でなくても，ホモトープになることがある．たとえば，図 9.1 に描かれた環状の集合は円にホモトープではあるが，同相ではない．

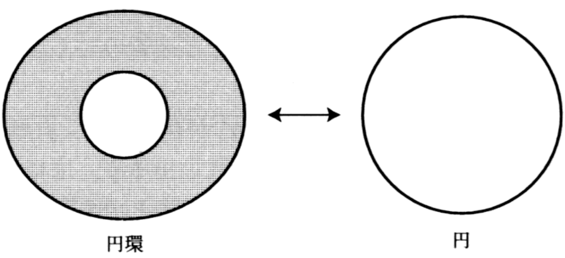


図 9.1　ホモトープであるが同相でない

ホモトピー不変量とはホモトピーによって保存される位相空間の性質である．第 9.3 節において，**基本群**と呼ばれる群を導入する．この群は空間のホモトピー的性質を表しており，それは 1 つのホモトピー不変量である．

ホモロジー理論は位相空間を**単体的複体**と呼ばれる組み合わせ論的対象として考察する．概略的に言えば n **単体**とは，n 次元実空間における多面体に相似な対象のことである．**単体的複体**とは，このような単体から特別な方法でつくられる (第 9.4 節参照)．一般位相空間は単体的複体に同相である部分から構成されているとき，これを空間の**単体分割**または**三角形分割**という．こ

の組み合わせ論的なアプローチは，前世紀の最後にアンリ・ポアンカレの先駆的な仕事において始められた．単体分割から，ホモロジー群と呼ばれるアーベル群の列をつくることができる．一般に，ホモトピーはホモロジーよりも強い不変量であるから，ホモトピー同値である 2 つの空間は同じホモロジー理論をもつ．これは第 9.4 節においてより正確に論じよう．

9.2 群論——アーベル群

代数的位相幾何学において用いられる代数的対象は主に群である．議論をさらに続ける前に，少し発展した群論を復習しなければならない．特に，有限生成アーベル群の構造定理が必要である．この定理は群の直積の構成に関係している．

定義 9.2.1 H と K を群とする．このとき，それらの**直積** $H \times K$ とは演算が $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$ によって定義されている集合 $\{(h,k) : h \in H, k \in K\}$ のことである．$H \times K$ が群になっていることを確かめるのは容易である．

次の補題において，以下の考察において最もかかわりのある直積に関する結果を要約することにする．証明はやさしいので演習として残しておく．

補題 9.2.1 $G = H \times K$ を群とするとき，次が成り立つ．

(1) $H_1 = H \times \{1\}, K_1 = \{1\} \times K$ はそれぞれ H と K に同型である G の正規部分群である．

(2) $H \times K$ が有限群であるための必要十分条件は H と K が有限群なることである．

(3) $H \times K$ がアーベル群であるための必要十分条件は H と K がアーベル群になることである．

上の補題 9.2.1 (1) より，H と K は $H \times K$ の正規部分群であると考えることができる．この構成の手順を反対にして，群 G の部分群から出発することにする．それらが補題 9.2.1 (1) の性質を満たせば，G はそれらの部分群の直積である．

補題 9.2.2 G を群とし，H, K を次の条件を満足している G の正規部分群であると仮定する．

(1) $G = HK$, すなわち，G はすべての積 $\{hk\,;\,h \in H, k \in K\}$ によって生成されている．

(2) $H \cap K = \{1\}$.

このとき，$G \cong H \times K$ が成り立つ．この場合，G はその部分群 H, K の直積であるという．

さて我々の注意をアーベル群にむけよう．補題 9.2.1 より，アーベル群の直積はそれ自身アーベル群である．群 G はただ 1 つの元 g によって生成されるとき，**巡回群**という．この場合，G はすべての異なった g のベキから構成される．明らかに，巡回群はアーベル群であり，ゆえに，巡回群の直積もまたアーベル群である（それらは巡回群であるとは限らない－演習問題参照）．

巡回群が無限位数をもてば，それは加法を演算とする整数 $\mathbb{Z}$ と同型である．それで，$\mathbb{Z}$ を無限巡回群を表すものとして用いる．巡回群の位数が n であれば，それは加法を演算とする n を法とする整数 $\mathbb{Z}_n$ に同型になる．それで，$\mathbb{Z}_n$ を位数 n の有限巡回群を表すものとして用いる．

G を群，n を自然数とするとき，G^n によって G の n 個のコピーの直積，すなわち，$G \times G \times \cdots \times G$ を表すことにする．このように表現すれば，$\mathbb{Z}^n$ は n 個の無限巡回群の直積である．無限巡回群の直積はアーベル群の構造において本質的な役割を果たすので，それらに特別な名称を与える．

定義 9.2.2 $\mathbb{Z}$ の n 個のコピーの直積 F を階数 n の**自由アーベル群**といい，rank $F = n$ と表す．すなわち，

$$F = \mathbb{Z} \times \cdots \times \mathbb{Z} = \mathbb{Z}^n.$$

F が自由アーベル群で，$g_1, \ldots, g_n$ を F の元とする．

$$F = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle$$

を満たすとき，$g_1, \ldots, g_n$ を F の**基底**という．

階数と基底という術語は，ベクトル空間において対応している術語を反映するように意図されている．この考えに従えば，次の補題が成り立ち，これはベクトル空間の性質を自由アーベル群に拡張したものとなっている．

補題 9.2.3 F を階数 n の自由アーベル群とするとき，次が成り立つ．

(1) 任意の基底を構成する元の個数は一意的で，n 個である．

(2) $g_1, \dots, g_n$ を基底とすれば，任意の $f \in F$ は一意的な表現をもつ．

$$f = g_1^{m_1} \cdots g_n^{m_n} \quad (m_i \in \mathbb{Z}).$$

(3) H が F の部分群ならば，H もまた自由アーベル群であり，$\operatorname{rank} H \leq \operatorname{rank} F$ が成り立つ．

自由という術語は自由アーベル群の次のようなカテゴリー的な定式化に由来している．この定理は，基底 $g_1, \dots, g_n$ をもつ自由アーベル群は $g_1, \dots, g_n$ によって生成されることのできる最も自由な（制限のない）アーベル群である，ということを主張している．

定理 9.2.1 $g_1, \dots, g_n$ をアーベル群 G の元とする．このとき，G が基底を $g_1, \dots, g_n$ とする自由アーベル群であるための必要十分条件は，アーベル群 H への各写像

$$g_1 \to H, \dots, g_n \to H$$

は G から H へのただ 1 つの準同型写像に拡張されることである．

アーベル群は，位数有限の元をもたないとき，**ねじれがない**という．すべての元が位数有限であるアーベル群を**ねじれ群**という．アーベル群 G において，位数有限であるすべての元は部分群をつくる．G がアーベル群であるから，これは必然的に正規部分群である．この部分群を**ねじれ部分群**といい，tG で表す．

補題 9.2.4 G がアーベル群ならば，位数有限であるすべての元は部分群をつくる．

（**証明**）$tG = \{g \in G; g$ の位数有限 $\}$ とおく．$1 \in tG$ であるから，tG は空集合ではない．$g_1, g_2 \in tG$ とする．このとき，$g_1^{n_1} = 1, g_2^{n_2} = 1$ を満たす整数 n_1, n_2 が存在する．すると，G はアーベル群であるから $(g_1 g_2)^{n_1 n_2} = (g_1)^{n_1}(g_2)^{n_2} = 1$. ゆえに，$g_1 g_2$ は有限位数であるから，$g_1 g_2 \in tG$. 同様にし

て，$(g_1^{-1})^{n_1} = (g_1^n)^{-1} = 1$, したがって，$g_1^{-1} \in tG$ となる．以上より，tG は部分群である． ■

群 G は有限個の生成系をもつとき，**有限生成**という．アーベル群に対して，次の定理が成り立つ．

補題 9.2.5 G が有限生成であるねじれアーベル群ならば，G は有限群である．

（**証明**）生成元が 2 個である場合に定理を証明する．一般の場合はこれより帰納法によって示される．

g_1, g_2 が G を生成すると仮定する．G はねじれ群であるから，g_1, g_2 はそれぞれ有限位数 n_1, n_2 をもつ．$g \in G$ とすると，g は $g = g_1^{t_1} g_2^{s_1} \cdots g_1^{t_k} g_2^{s_k}$ と表される．G はアーベル群だから，g_1 をすべて一緒にし，g_2 もすべて一緒にすることができるので

$$g = g_1^t g_2^s \quad (t, s \in \mathbb{Z})$$

と表すことができる．これはすべての $g \in G$ について成り立つので，G の元の個数は t の選び方の数と s の選び方の数の積によって抑えられる．g_1 の位数は n_1，g_2 の位数は n_2 であるから，この積は $n_1 n_2$ である．ゆえに，$|G| \leq n_1 n_2$ であるから，G は有限である． ■

アーベル群ではない群に対して，対応する命題は成り立たない．すなわち，すべての元は有限位数でかつ無限群であるような有限生成である群が存在する．すべての元の位数がある整数 m 以下であるような n 個の元によって生成される群は有限群かどうかを問う問題を**バーンサイドの問題**という．一般には，これに対する否定的な答えがある．この問題の議論については Gupta による概説的な論文 [G] を引用しておく．

これまで説明してきた準備のもとに，有限生成アーベル群の基本定理を述べよう．一連の補題によってその証明の概略をたどってみよう．しかしながら，ほとんどの証明の詳細は省略する．非常に理解しやすい完全な議論はロットマンの本 [Ro] にある．一連の補題を用いた証明の後で，この定理を用いた例をあげよう．

定理 9.2.2（有限生成アーベル群の基本定理）G を有限生成アーベル群とする．そのとき，G は有限階数の自由アーベル群と素数ベキを位数とする有限個の巡回群との直積に（因子の順序を除いて）一意的に分解される．

G の自由アーベル群の階数は G の不変量であり，**ベッチ数**と呼ばれる．

前に説明したように，補題 9.2.6 から補題 9.2.10 までは定理 9.2.2 の証明を概略している．

補題 9.2.6 G が有限生成アーベル群ならば，G は巡回群の直積である．

補題 9.2.7 G がねじれのない有限生成アーベル群ならば，G は有限階数の自由アーベル群である．

補題 9.2.8 G が有限生成アーベル群ならば，$G = tG \times$ (自由アーベル群) と表される．

補題 9.2.9 G が有限アーベル群ならば，G は位数が素数ベキの部分群の直積である．

p を素数とするとき，そのすべての元の位数が p のベキとなっている群を **p-群**という．ラグランジュの定理より，明らかに，位数が素数ベキの群は p-群である．

補題 9.2.10 G が有限アーベル群でかつ p-群ならば，G は巡回 p-群の直積である．さらに，この分解は因子の順序を除いて一意的である．

さて，定理を用いた例をあげよう．

例 9.2.1 ベッチ数 3 でねじれ群の位数 180 のすべてのアーベル群を分類しよう．

G をそのような群とすると，ベッチ数 3 だから

$$\begin{aligned} G &\cong tG \times (\text{自由アーベル群}) \\ &= tG \times \mathbb{Z}^3. \end{aligned}$$

$|tG| = 180$ だから，位数 180 のすべての有限アーベル群を分類しなければならない．

180 の素因数分解は $2^2 3^2 5$ である．したがって，位数が素数ベキの巡回群への可能な分解は次のようである．

(1) $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$.

(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5$.

(3) $\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

(4) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

2 つの部分を一緒にすると，指定された性質をもつ群は正確に 4 つの可能なアーベル群が存在することがわかる．すなわち，

(1) $\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}^3$.

(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}^3$.

(3) $\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}^3$.

(4) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}^3$. □

トポロジーにもどる前に，群論からもう 1 つの考えに言及しておこう．アーベル群 G では，任意の元 $g, h \in G$ に対して積 $ghg^{-1}h^{-1}$ は常に 1 である．一般にこのことは成り立たない．G がアーベル群でないとき，$ghg^{-1}h^{-1} = 1$ $(g, h \in G)$ ならば，$gh = hg$ である．このとき，g と h は**可換**（**交換可能**）であるという．G におけるこの種類の積の集合は，この群がいかにアーベル群から離れているかを表している．このことをもっと注意深く考察してみよう．

定義 9.2.3　G を群とする．$g, h \in G$ とするとき，それらの積 $ghg^{-1}h^{-1}$ を $[g, h]$ で表し，**交換子**という．明らかに，g と h が可換であるための必要十分条件はそれらの交換子が 1 になることである．

G のすべての交換子によって生成される G の部分群を G の**交換子部分群**といい，$[G, G]$ あるいは G' によって表す．明らかに G がアーベル群であるための必要十分条件はその交換子部分群が自明になることである．

定理 9.2.3　G を群とする．このとき，G' は G の正規部分群であり，その剰余群 G/G' はアーベル群である．さらに，H が G の正規部分群で，かつ G/H がアーベル群ならば，$G' \subset H$ が成り立つ．

したがって，G/G' は可換となる最大の G の剰余群である．G/G' を G の**アーベル化**と呼び，これを G^{ab} によって表す．

（**証明**）定義によって，G' は部分群である．これが正規部分群であることを示さなければならない．$x \in G$ として，次を考察する．

$$\begin{aligned} x^{-1}[g,h]x &= x^{-1}ghg^{-1}h^{-1}x \\ &= x^{-1}gxx^{-1}hxx^{-1}g^{-1}xx^{-1}h^{-1}x \\ &= [x^{-1}gx, x^{-1}hx]. \end{aligned}$$

ゆえに，交換子のすべての共役は再び交換子である．したがって，G' は正規部分群である．

剰余群 G/G' を考える．$u = gG', v = hG'$ とおく．このとき，$[g,h] \in G'$ であるから，$uvu^{-1}v^{-1} = ghg^{-1}h^{-1}G' = [g,h]G' = G'$. ところが，これは G/G' において交換子 $[u,v] = uvu^{-1}v^{-1} = 1$ を意味している．ゆえに，G/G' はアーベル群である．

最後に，G/H がアーベル群であると仮定する．$g, h \in G$ として，剰余類 gH, hH を考える．すると，G/H はアーベル群であるから

$$ghH = hgH.$$

このとき，$ghg^{-1}h^{-1}H = H$. すなわち，$[g,h]H = H$ である．このことは，すべての交換子に対して $[g,h] \in H$ であることを意味しているから，$G' \subset H$ となる． ■

9.3 ホモトピーと基本群

ホモトピーという概念を導入し，これより最初の代数的不変量である基本群をつくる．X, Y が位相空間で，$f: X \to Y, g: X \to Y$ を連続写像とする．直感的に，f が g に連続的に変形できるとき，f は g にホモトープであるという．このことを，正確に論じよう．この章の以下において，$I = [0,1]$ を実直線 $\mathbb{R}$ 上の単位区間とする．X, Y を位相空間とする．このとき，O_x, O_y をそれぞれ X, Y の開集合として，すべての $O_x \times O_y$ のかたちの集合を開集合の基底として直積 $X \times Y$ を位相空間にすることができる（演習問題参照）．

定義 9.3.1　X, Y が位相空間で，$f: X \to Y, g: X \to Y$ を連続写像とする．連続写像 $H: X \times I \to Y$ が存在し，任意の $x \in X$ に対して $H(x,0) = f(x)$, $H(x,1) = g(x)$ を満たすとき，f は g に**ホモトープ**であるという．写像 H を**ホモトピー**という．このとき，g もホモトピー $H_1(x,t) = H(x, 1-t)$ によって f にホモトープであるから，一般に f と g は**ホモトープ**であるという．

この定義を理解するために, 区間 I を**時間媒介変数空間**として考える．こうすることによって，各点 $t \in [0,1]$ で，写像 $H_t(x) = H(x,t)$ を時間 t における X から Y への連続写像と考えることができる．時間 $t = 0$ のとき $H_0(x) = f(x)$ であり，一方，時間 $t = 1$ のとき $H_1(x) = g(x)$ である．$H(x,t)$ の連続性は時間とともに連続的に変形することを表している．

例として，$X = [a,b] \subset \mathbb{R}$, $Y = \mathbb{R}^2$ とする．このとき，f, g は $\mathbb{R}^2$ における道を表す．それらがホモトープであれば，図 9.2 のように図解することができる．点線で描かれた道は中間の時間における道を表す．

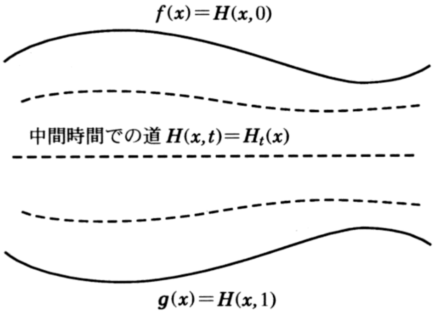


図 9.2　道のホモトピー

f が g にホモトープであれば，g は f にホモトープであることを述べた．ゆえに，ホモトープは X から Y への連続写像の集合上の対称な関係である．さらに，それは推移的でもある．すなわち，f が g にホモトープで，g が h にホモトープであれば，f が h にホモトープである．これを見るために，H_0 を f から g へのホモトピー，H_1 を g から h へのホモトピーとする．この

とき，

$$H_2(x,t) = H_0(x,2t) \quad (0 \leq t \leq \frac{1}{2}),$$
$$H_2(x,t) = H_1(x,2t-1) \quad (\frac{1}{2} \leq t \leq 1)$$

によって定義される写像 $H_2 : X \times I \to Y$ は f から h へのホモトピーである．明らかに，1 つの連続写像は自分自身にホモトープであるから，ホモトープは X から Y への連続写像の集合上における同値関係である．この関係による同値類は**写像のホモトピー類**と呼ばれる．

ホモトピーの概念を写像から全体の空間へ拡張しよう．

定義 9.3.2 X, Y を位相空間とする．連続写像 $f : X \to Y, g : Y \to X$ が存在して，その合成写像 gf は X 上の恒等写像にホモトープであり，fg は Y 上の恒等写像にホモトープであるとき，X と Y は, **ホモトピー同値**または**ホモトープ**であるという．直感的に言うと，2 つの空間は連続的に変形できる（お互いにつまんだり，縮めたりして）ならばホモトープであるといえる．明らかに，同相な空間はホモトープであるが，同相でないホモトープな空間が存在する．1 つの例は図 9.1 に描かれていた．環状の集合は円にホモトープであるが，同相ではない．写像の場合と同様に，ホモトープは位相空間上の同値関係である．したがって，**空間のホモトピー類**が定義される．**ホモトピー不変量**はホモトピーによって不変な位相的性質のことである．このようにして，1 つのホモトピー類のなかのすべての空間は同じホモトピー不変量をもつ．

位相空間はそれが 1 点にホモトープであるとき，**収縮可能**であるという．たとえば，$\mathbb{R}^2$ における単位円盤の内部は収縮可能である．すべての収縮可能な空間はお互いにホモトープである．

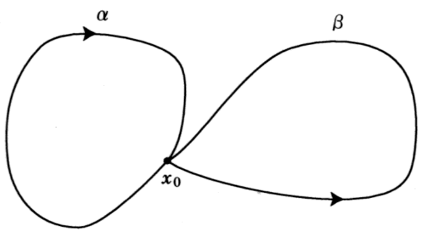
さて，次に空間の基本群を構成する．これは空間の代数的ホモトピー不変量となる．一般位相空間 X における**道**とは連続写像 $\alpha : [0,1] \to X$ のことである．$x_0 \in X$ とする．$\alpha(0) = \alpha(1) = x_0$ を満たす道 α, すなわち，出発点と終点が同じ点 x_0 である道 α を**ループ**または**閉じた道**という．

x_0 を X の固定した点とし，x_0 を基点とするすべてのループの集合を $C(X, x_0)$ で表す．$C(X, x_0)$ におけるホモトピー類に演算を定義して群を構成する．

はじめに，α, β を x_0 を基点とするループとする．それらの積 $\alpha\beta$ を，最初に α の上を行き (実際は α の像の上), 次に β の上を行くループとして定義する．関数として，これは次のように表現される．

$$\alpha\beta(t) = \alpha(2t) \qquad (0 \leq t \leq \frac{1}{2}),$$
$$\alpha\beta(t) = \beta(2t-1) \ (\frac{1}{2} \leq t \leq 1).$$

図 9.3 はこれを説明している．



$\alpha\beta$ は最初に α の上を，次に β の上を行く

図 9.3　ループの積

x_0 を基点とするループの積はホモトピーによって保存される．すなわち，α が α_1 にホモトープ，β が β_1 にホモトープならば，$\alpha\beta$ は $\alpha_1\beta_1$ にホモトープである．さらに，この積はホモトピーを除いて結合的である．このことは，α, β, γ を x_0 を基点とするループとするとき，$(\alpha\beta)\gamma$ は $\alpha(\beta\gamma)$ にホモトープであることを意味している．上で述べたことをまとめておこう．

補題 9.3.1　α, β, γ を x_0 を基点とするループとするとき，次が成り立つ．

(1) α が α_1 にホモトープで，β が β_1 にホモトープならば，$\alpha\beta$ は $\alpha_1\beta_1$ にホモトープである．

(2) $(\alpha\beta)\gamma$ は $\alpha(\beta\gamma)$ にホモトープである．

α を x_0 を基点とするループとし，$[\alpha]$ をそのホモトピー類とする．$[\alpha]$ は α にホモトープである x_0 を基点とするすべてのループからなる．$[\alpha][\beta] = [\alpha\beta]$ と定義する．すなわち，2 つのループのホモトピー類の積は，それらの代表元の積のホモトピー類である．補題 9.3.1 より，これはホモトピー類の集合の上に矛盾なく定義されていることがわかる．さらに，この補題の後半の部

分より，この積はホモトピー類の集合の上の演算として結合的であることがわかる．x_0 を基点とするループのホモトピー類の集合を $\prod_1(X,x_0)$ で表す．このようにして，$\prod_1(X,x_0)$ は矛盾なく定義された結合的な演算をもつ．

e を x_0 の恒等的なループとする．すなわち，すべての $t \in [0,1]$ 対して $e(t)=x_0$. このとき，x_0 を基点とする任意のループに対して $e\alpha=\alpha e=\alpha$. ゆえに，$[e][\alpha]=[\alpha][e]=[\alpha]$ が成り立つから，$[e]$ は $\prod_1(X,x_0)$ における単位元である．最後に，α を x_0 を基点とするループとし，$\alpha^{-1}(t)=\alpha(1-t)$ と定義する．すなわち，α^{-1} は逆方向に道 α を行くループである．$\alpha\alpha^{-1}$ と $\alpha^{-1}\alpha$ は e にホモトープであることを示すことができるので，$[\alpha\alpha^{-1}]=[\alpha^{-1}\alpha]=[e]$ を得る．したがって，$\prod_1(X,x_0)$ の各元は逆元をもつ．以上より，$\prod_1(X,x_0)$ は矛盾なく定義された演算をもち，この演算は結合的であり，単位元をもち，任意の元に対して逆元をもつことがわかった．ゆえに，$\prod_1(X,x_0)$ は群を構成する．

定理 9.3.1　x_0 を基点とするループのホモトピー類の集合 $\prod_1(X,x_0)$ は演算 $[\alpha][\beta]=[\alpha\beta]$ によって群となる．この群を x_0 **に基点をもつ** X **の基本群**という．

上の定義は基点 x_0 に依存しているが，多くの場合この制限を除去することができる．$x_1 \in X$ とし，X において x_0 から x_1 への道，すなわち，連続関数 $p:[0,1]\to X$, $p(0)=x_0, p(1)=x_1$ があると仮定する．このとき，$\prod_1(X,x_0)$ は $[\alpha]\to[p^{-1}\alpha p]$ によって定義される同型写像によって，$\prod_1(X,x_1)$ と同型になる．これは図 9.4 において示されている．

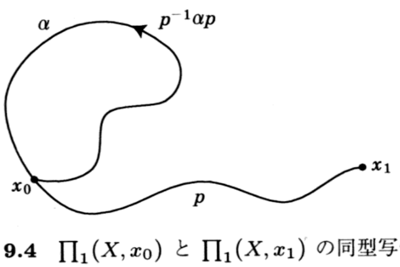


図 9.4　$\prod_1(X,x_0)$ と $\prod_1(X,x_1)$ の同型写像

定理 9.3.2　x_0, x_1 を空間 X の点とする．このとき，x_0 と x_1 が適当な道 p

によってつながっていれば，$\prod_1(X, x_0) \cong \prod_1(X, x_1)$ となる．

位相空間は，任意の 2 点 $x_0, x_1 \in X$ が適当な道によって結ぶことができるとき，**弧状連結**であるという．この定義を使えば，次のような定理 9.3.2 の重要な系が得られる．

系 9.3.1　X が弧状連結ならば，任意の 2 点 $x_0, x_1 \in X$ に対して $\prod_1(X, x_0) \cong \prod_1(X, x_1)$ が成り立つ．したがって，この場合 X に対して定義される基本群はただ 1 つである．これを X の**基本群**と呼び，$\prod_1(X)$ で表す．

この節の残りは，弧状連結空間のみを考察する．

空間が収縮可能ならば $\prod_1(X) = \{1\}$ である．逆に，$\prod_1(X) = \{1\}$ ならば X におけるすべてのループは 1 点に収縮する．このような空間を**単連結**という．いくつか例をあげよう．

例 9.3.1

(1) $\mathbb{R}^2$ における単位円盤，あるいは，$\mathbb{R}^n$ における球体は収縮可能であり，したがって，単連結である．

(2) $n > 1$ のとき，n 次元球面 $S^n \subset \mathbb{R}^{n+1}$ は単連結であるが，収縮可能ではない．ただし，$n \geq 0$ に対して，n 次元球面とは $S^n = \{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1}\,;\, x_1^2 + x_2^2 + \cdots + x_{n+1}^2 = 1\}$ である．　□

例 9.3.2　円 $S^1 \subset \mathbb{R}^2$ を考える．この円周上の基点と道に対する向きを固定する．この円のまわりをまわっているのではない任意のループは 1 点にホモトープである．あるループが 1 つの円のまわりを 1 回よりは多くまわり，しかし 2 回はまわっていないループはちょうど 1 回まわっているループにホモトープである．一般に，あるループが円のまわりをちょうど n 回以上まわっているループにホモトープならば，このループは回転数が n であるという．同じ回転数をもつすべてのループはホモトープである．

この考えによれば，円上のループのホモトピー類の集合は，回転数 $n = 0, 1, 2, \cdots$ をもつループとそれらの逆元からなる．回転数 n のループの逆元は反対向きに n 回回転する．このとき，これは回転数 $(-n)$ をもつという．さらに，ループの乗法は回転数の単なる加法である．このようにして，ホモトピー類

の乗法は整数の加法のように振る舞う．したがって，円の基本群は無限巡回群であることがわかる．

$$\prod_1(S^1) = \mathbb{Z}.$$

例 9.3.3 図 9.5 のようなトーラスを考える．

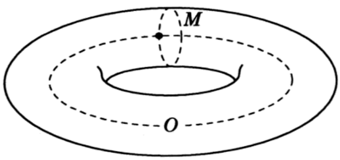


図 9.5 トーラス

一般のループは内側の円 M をまわっているループと外側の円 O をまわっているループにホモトープである．このようなループは M と O のまわりをまわる回転数をもつ．さらに，M と O のまわりをまわるループは可換である．したがって，$\prod_1(T)$ は階数 2 の自由アーベルである．すなわち，

$$\prod_1(T) = \mathbb{Z} \times \mathbb{Z}.$$

この結果は次のように考えても得られる．トーラス T は 2 つの円の直積空間 $T = S^1 \times S^1$ と考えることができる．X, Y が弧状連結空間ならば，

$$\prod_1(X \times Y) = \prod_1(X) \times \prod_1(Y).$$

したがって，

$$\prod_1(T) = \prod_1(S^1) \times \prod_1(S^1) = \mathbb{Z} \times \mathbb{Z}.$$ □

最後に，すべての基本群がアーベル群とは限らないということを示す例をあげる．

例 9.3.4 図 9.6 におけるように，$\mathbb{R}^2$ における 8 の字の図形を考える．

トーラスの場合に見たように，あるループは 1 つの円のまわりをまわるループともう 1 つの円をまわるループの直積にホモトープである．しかし，この曲線は平面的でかつ 1 次元であるから，上の円をまわるループは下の円をま

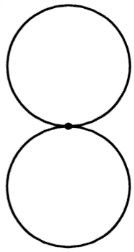


図 9.6　2 つの円の花束

わるループと可換ではない．α を上の円を与えられた向きに 1 回まわるループで，β を下の円を与えられた向きに 1 回まわるループとする．そのとき，一般のループは次の形のループにホモトープである．

$$\alpha^{n_1}\beta^{m_1}\cdots\alpha^{n_k}\beta^{m_k} \quad (n_1, m_1, \ldots, n_k, m_k \in \mathbb{Z}).$$

このようなループは α, β による**語**と呼ばれ，対応している群は階数 2 の**自由群**である．この群は非可換であり，階数 2 の自由アーベル群と混同されるべきではない．ここでは，これ以上これらの群に立ち入らない．詳細については，[Ro] を参照せよ．

一般に，1 点で接触している n 個の円からなる空間図形は n 個の**円の花束**と呼ばれている．それから得られる基本群は階数 n の**自由群**である．　□

基本群はホモトピー不変量である．特に，X, Y を弧状連結空間で，$h : X \to Y$ を連続写像とすれば，X における任意のループ α に対して，$h(\alpha)$ は Y におけるループである．したがって，h は $h^*[\alpha] = [h(\alpha)]$ によって写像 $h^* : \prod_1(X) \to \prod_1(Y)$ を定義する．この写像は群の準同型写像であることがわかる．

定理 9.3.3 X, Y を弧状連結空間で，$h : X \to Y$ を連続写像とすれば，$h^*[\alpha] = [h(\alpha)]$ によって定まる写像 $h^* : \prod_1(X) \to \prod_1(Y)$ は群の準同型写像である．h が同相写像ならば，h^* は同型写像である．さらに，X, Y がホモトープならば，$\prod_1(X)$ は $\prod_1(Y)$ に同型である．

例 9.3.5 図 9.1 における環状の集合 A を考える．A は円にホモトープであるから，次が成り立つ．

$$\prod_1(A) = \prod_1(S^1) = \mathbb{Z}.$$

すべての群は 2 次元の複体の基本群として考えることができることに言及しておこう．したがって，抽象的な意味で，群論の研究は実際基本群の研究であるということができる．このことについての完全な議論は文献 [Ro] を参照するとよい．

第 7 章で導入した体のガロア理論に類似の，空間の基本群に付随したガロア理論がある，ということに言及してこの節を閉じることにする．これを簡潔に説明しよう．

定義 9.3.3 B, X を弧状連結空間とする．写像 $p: B \to X$ が存在して，任意の $x \in X$ に対して，x のある開近傍 U が存在し，$p^{-1}(U)$ の各成分は p のもとで U に同相であるとき，B は X の**被覆空間**といい，p を**被覆写像**という．

$p: B \to X$ は準同型写像 $p^*: \prod_1(B) \to \prod_1(X)$ を定義する．被覆写像の条件はこの写像が 1 対 1 であることを意味しているので，$\prod_1(B)$ は $\prod_1(X)$ の部分群と考えることができる．さて，x が X の特別な基点とすれば，いくつかの点（無限も可）b_i が x に写像される．群 $\prod_1(B, b_i)$ はすべて同型であり，$\prod_1(X)$ における共役な部分群の完全集合に対応している．逆に，$\prod_1(X)$ における共役な部分群の完全集合 $\{H_i\}$ が与えられると，$\prod_1(B) \cong H_i$ を満たす弧状連結な被覆空間 B をつくることができる．自明な部分群 $\{1\}$ に対応している X の単連結被覆空間 V は X の**普遍被覆空間**と呼ばれる．以上の結果を要約しておこう．これらは被覆空間のガロア理論として知られている，

定理 9.3.4

(1) B を，被覆写像を p とする弧状連結空間 X の弧状連結被覆空間とする．このとき，次が成り立つ．

(i) $p^*: \prod_1(B) \to \prod_1(X)$ は単射であり，したがって，$\prod_1(B)$ は $\prod_1(X)$ の部分群と考えることができる．

(ii) $x \in X, p^{-1}(x) = \{b_i\} \subset B$ とすると，$p^*(\prod_1(B, b_i))$ は $\prod_1(X)$ における共役な部分群の完全集合である．

(2) $\prod_1(X)$ における共役な部分群の完全集合 $\{H_i\}$ が与えられると，$\prod_1(B) \cong H_i$ を満たす X の弧状連結な被覆空間 B が存在する．

9.4　ホモロジー理論と三角形分割

n 次元ユークリッド空間 $\mathbb{R}^n$ において，標準的な単位ベクトルを $\boldsymbol{e}_1 = (1,0,\ldots,0), \boldsymbol{e}_2 = (0,1,\ldots,0),\ldots,\boldsymbol{e}_n = (0,0,\ldots,1)$ とする．$\Delta_0 = (0,0,\ldots,0)$ を原点とし，$1 \leq q < n$ に対して，Δ_q を $\boldsymbol{e}_1,\ldots,\boldsymbol{e}_{q+1}$ の**凸胞体**とする．この集合は $\mathbb{R}^n$ における次のように表されるベクトルの集合である．

$$\{u \in \mathbb{R}^n \ : u = a_1\boldsymbol{e}_1 + \cdots + a_{q+1}\boldsymbol{e}_{q+1},$$

$$a_i \in \mathbb{R},\ 0 \leq a_i \leq 1,\ 0 \leq i \leq q+1,\ \sum_{i=1}^{q+1} a_i = 1\}.$$

Δ_0 は 1 点，Δ_1 は単位区間，Δ_2 は三角形，Δ_3 は四面体等々．$\mathbb{R}^n$ における q **次元単体**とは Δ_q に同相である任意の部分集合のことである．一般位相空間において，q 次元単体とは Δ_q に同相である任意の部分集合 $D \subset X$ のことである．

これらの単体から代数的不変量を構成するためには，それらに向きを付けなければならない．$P_0, P_1,\ldots,P_n$ を $\mathbb{R}^n$ における $n+1$ 個の独立な点とする．独立であるという意味はベクトル $\boldsymbol{u}_1 = \overrightarrow{P_0P_1}, \boldsymbol{u}_2 = \overrightarrow{P_0P_2},\ldots,\boldsymbol{u}_n = \overrightarrow{P_0P_n}$ が一次独立であるということである．**向きのついた 0 単体**とは 1 点であり，したがって，Δ_0 に同相である．**向きのついた 1 単体**とは向きのある線分 P_0P_1 のことで，$P_0P_1 = -P_1P_0$ と約束する．これは向きのついた Δ_1 に同相である．

高次元の向きのついた単体を定義するためには置換に関するある考えを必要とする．置換 $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ はそれが偶数個の互換の積に分解されるとき**偶置換**といい (演習問題 7.18 参照)，そうでないとき**奇置換**であるという．これは巡回置換の積に分解したとき，各巡回置換の長さより 1 つ小さい数の和が偶数であるか奇数であるかによって偶置換，奇置換と定義するのと同値である (演習問題 7.18 参照)．たとえば，$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$ は偶置換であり，

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2)$ は奇置換である．また，$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\,2\,3)(4\,5)$ は奇置換である．なぜなら，$(1\ 2\ 3)$ の長さより 1 つ小さい数は 2 であり，$(4\ 5)$ の長さより 1 つ小さい数は 1 であるから，その和は 3 で奇数である．

さて，**向きのついた 2 単体**とは Δ_2 に同相である $\mathbb{R}^n$ の部分集合である．したがって，あらかじめ定められた 3 つの頂点についての向きをもつ三角形に同相である．このことは 3 つの点の有向列 $P_0P_1P_2$ を与えることと同値である．$P_1P_2P_0$ は $P_0P_1P_2$ と同じ向きであり，$P_0P_2P_1$ はその反対の向きを与える．一般に，置換 $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ が偶置換ならば $P_0P_1P_2 = P_iP_jP_k$ であり，奇置換ならば $P_0P_1P_2 = -P_iP_jP_k$ である．したがって，

$$P_0P_1P_2 = P_1P_2P_0 = P_2P_0P_1 = -P_0P_2P_1 = P_1P_0P_2 = -P_2P_1P_0.$$

向きのついた q 単体とは頂点についてあらかじめ定められた向きをもつ Δ_q に同相である $\mathbb{R}^n$ の部分集合である．このことは単体を，上で見たように，対応している置換が偶置換か奇置換かによって $P_0P_1\ldots P_q = \pm P_{i_1}\ldots P_{i_q}$ と約束したとき，次のような有向点列として表現することと同値である．向きのついた q 単体を $P_0P_1\ldots P_q$ のような点列として表現しよう．一般の位相空間における向きのついた q 単体とは，あらかじめ定められた向きをもつ $\mathbb{R}^n$ の向きのついた q 単体の同相な像である．

q 単体 $P_0P_1\ldots P_q$ に対して，点 P_i を除くことによって得られる $q-1$ 単体を
$P_0P_1\ldots\overline{P_i}\ldots P_q$ で表す．このとき，次のように定義する．

定義 9.4.1 $P_0P_1\ldots P_q$ を向きのついた q 単体とする．$i=0,\ldots,q$ に対して，

$$(-1)^iP_0P_1\ldots\overline{P_i}\ldots P_q$$

によって与えられる向きのついた $(q-1)$ 単体をその**辺**という．したがって，q 単体は $(q+1)$ 個の辺をもつ．

たとえば，向きのついた 3 単体 $P_0P_1P_2P_3$ は 4 個の辺 $P_1P_2P_3, -P_0P_2P_3, P_0P_1P_3, -P_0P_1P_2$ をもつ．

0 単体に対して，その境界を空なる単体として定義し，これを 0 によって表す．ゆえに，$\partial_0(P_0)=0$. $q \geq 1$ に対して，q 単体 $P_0P_1\ldots P_q$ の**境界** ∂_q をその辺の形式的な和として定義する．

定義 9.4.2 $q \geq 1$ のとき，$P_0P_1\ldots P_q$ を向きのついた q 単体とする．このとき，その**境界** ∂_q は次で定義される．

$$\partial_q(P_0P_1\ldots P_q)=\sum_{i=0}^{q}(-1)^i P_0P_1\ldots\overline{P_i}\ldots P_q.$$

最初の 4 つの次元について，次のことが成り立つ．

(1) $\partial_0(P_0)=0$.
(2) $\partial_1(P_0P_1)=P_1-P_0$.
(3) $\partial_2(P_0P_1P_2)=P_1P_2-P_0P_2+P_0P_1$.
(4) $\partial_3(P_0P_1P_2P_3)=P_1P_2P_3-P_0P_2P_3+P_0P_1P_3-P_0P_1P_2$.

境界作用素を辺の形式的和に適用するとき，それは加法的に行なわれる．たとえば，

$$\begin{aligned}\partial_1(P_1P_2-P_0P_1) &= \partial_1(P_1P_2)-\partial_1(P_0P_1)\\ &= P_2-P_1-(P_1-P_0)=P_2-2P_1+P_0.\end{aligned}$$

次の結果はホモロジー群の構成に対して重要である．この補題は境界作用素を 2 回施すと常に 0 になることを主張している．

補題 9.4.1 任意の q 単体に対して，$\partial_{q-1}\partial_q=0$ が成り立つ．したがって，q 単体の任意の形式的な和に $\partial_{q-1}\partial_q$ を加法的に適用すれば常に 0 となる．

（**証明**）2 単体に対して補題を示し，3 単体に対する計算は演習として残しておこう．また，一般の場合は同様にすればできる．

$P_0P_1P_2$ を 2 単体とすると，

$$\begin{aligned}\partial_1\partial_2(P_0P_1P_2) &= \partial_1(P_1P_2 - P_0P_2 + P_0P_1)\\ &= \partial_1(P_1P_2) - \partial_1(P_0P_2) + \partial_1(P_0P_1)\\ &= P_2 - P_1 - P_2 + P_0 + P_1 - P_0\\ &= 0.\end{aligned}$$

■

多面体のような $\mathbb{R}^n$ における多くの幾何的な図形は，単体からうまい方法でつくることができる．これらの図形は**単体的複体**と呼ばれる．これは以下のように形式的に定義される．はじめに，q 単体に対して，その部分単体を向きに関係なくすべての辺，辺のすべての辺，辺の辺のすべての辺，等々として定義する．したがって，たとえば $P_0P_1P_2P_3$ の部分単体の集合は次のようである．

$$P_1P_2P_3,\ P_0P_2P_3,\ P_0P_1P_3,\ P_0P_1P_2$$

$$P_0P_1,\ P_0P_2,\ P_0P_3,\ P_1P_2,\ P_1P_3,\ P_2P_3,\ \ P_0,\ P_1,\ P_2,\ P_3.$$

定義 9.4.3　$\mathbb{R}^n$ における単体的複体とは次の条件を満たす集合である．

(1) それは向きのついた単体の和集合である．$\mathbb{R}^n$ において可能な単体の最大次元は $n-1$ であることに注意せよ．

(2) 各点は有限個の単体に属する．

(3) 2 つの異なった（向きを除いて）単体の共通集合は空集合であるか，または単体の 1 つになるか，またはそれら 2 つの部分単体の 1 つになる．

図 9.7 の図形 (A) は $\mathbb{R}^2$ における単体的複体であり，一方 (B) は (3) に反するのでそうではない．

次にこの定義を一般位相空間に拡張しよう．前に指摘したように，一般位相空間 X において，向きのついた q 単体はあらかじめ定められた向きのある $\mathbb{R}^{n+1}$ のなかの向きのついた q 単体の同位相な像である．その辺と部分単体は X の対応している辺と部分単体に移される．一般に可能である単体の次元は有界ではないということに注意しよう．

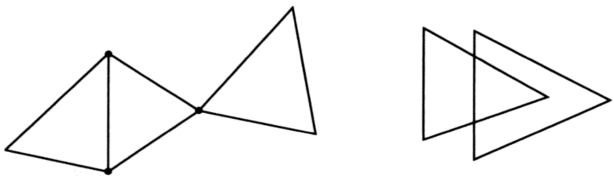


図 9.7　単体的複体

定義 9.4.3′ X を位相空間とする．X における**単体的複体**とは次の条件を満たす部分集合 Y のことである．

(1) それは向きのついた単体の和集合である ($\mathbb{R}^n$ との違いは，可能な単体の最大次元はないことに注意せよ).

(2) 各点は有限個の単体に属する．

(3) 2 つの異なった（向きを除いて）単体の共通集合は空集合であるか，または単体の 1 つになるか，またはそれら 2 つの部分単体の 1 つになる．

Y の単体について最大次元 q が存在すれば，Y は q **次元単体的複体**と呼ばれる．

X が単体的複体として構成されている部分集合の族をもつとき，X は**単体分割**をもつまたは X は**三角形分割**をもつという．空間 X の単体分割から，代数的不変量を構成する．$\mathbb{R}^n$ における 2 つの三角形分割の例をあげよう．

例 9.4.1 S^1 を $\mathbb{R}^2$ における単位円とする．このとき，1 次元単体としての三角形分割は，図 9.8 に示すとおりである．0 単体は P_0, P_1, P_2 であり，1 単体は P_0P_1, P_1P_2, P_2P_0 である． □

例 9.4.2 T をトーラスとする．平面において，図 9.9 のように，辺を同一視した長方形によって T を表すことができる．トーラスを復元するためには，上辺を同一視した底辺に重ねて円筒にし，それから円筒の上にできる円と下にできる円を同一視すればよい．

このとき，トーラスの三角形分割は図 9.10 のように描くことができる．ここで，例 9.4.1 の円のように有界な円を三角形分割し，結果として三角形による分割を得る． □

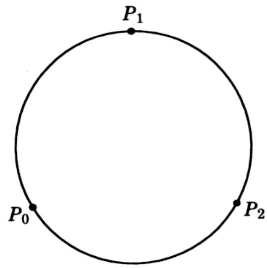


図 9.8 円の三角形分割

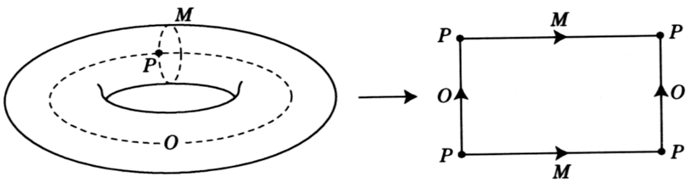


図 9.9 平面のトーラス

三角形分割から群を構成する．考えている空間は単体複体であり，さらに，次の有限性についての条件も付け加える．すなわち，各次元 q について，X には有限個の q 単体複体が存在する．この条件は本質的ではなく，我々の考えている応用と代数学の基本定理の証明に対しては必要なものである．そこで，X は上の条件を満たしている単体複体と仮定する．$n = 0, 1, 2, \ldots$ に対して，$C_n(X)$ を単体の数に等しい階数の自由アーベル群とする．この群を n **鎖加群**と呼ぶ．$C_n(X)$ の元は n **鎖**と呼ばれる．X は t 個の n 単体 $D_n^1, D_n^2, \ldots, D_n^t$ をもつと仮定する．このとき，これらを群 $C_n(X)$ の基底と考える．したがって，$C_n(X)$ の元は次のような和として表される．

$$m_1 D_n^1 + m_2 D_n^2 + \cdots + m_t D_n^t \quad (m_i \in \mathbb{Z}) \tag{9.4.1}$$

($C_n(X)$ はアーベル群であるから，通常は演算として加法の記号を用いることに注意せよ)．したがって，n 鎖は (9.4.1) のような形の和として表される．

D_n^k を X における n 単体とするとき，前に定義したように，その境界 $\partial_n D_n^k$ は $(n-1)$ 単体の和である．ゆえに，$\partial_n D_n^k \in C_{n-1}(X)$ である．この境界作用素 ∂_n は基底のすべての元で定義されているので，全体の群の準同型写像

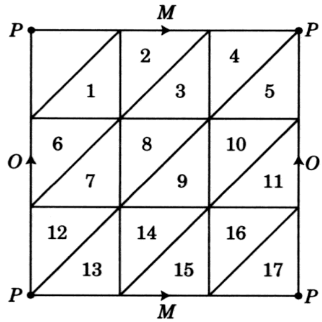


図 9.10　トーラスの三角形分割

へと拡張できる．したがって，**境界準同型写像**

$$\partial_n : C_n(X) \to C_{n-1}(X)$$

は

$$\partial_n(m_1 D_n^1 + m_2 D_n^2 + \cdots + m_t D_n^t) = m_1 \partial_n(D_n^1) + \cdots + m_t \partial_n(D_n^t)$$

によって与えられる．

補題 9.4.1 より，$\partial_{n-1}\partial_n : C_n(X) \to C_{n-2}(X)$ は常に自明な準同型写像である．

∂_n の核はその境界が 0 となるすべての n 単体からなる．これらの元を n **次元輪体**と呼ぶ．この核は $C_n(X)$ の部分群であり，n **次元輪体群**と呼び，$Z_n(X)$ によって表される．

∂_{n+1} による $C_{n+1}(X)$ から $C_n(X)$ への像は，n **次元境界群**と呼び，$B_n(X)$ によって表される．したがって，n 鎖はそれが $(n+1)$ 鎖の境界ならば $B_n(X)$ に属する．$\partial_n\partial_{n+1} = 0$ という関係より，$B_n(X)$ は $Z_n(X)$ の部分群であることがわかる．すなわち，任意の n 境界は n 輪体である．

すべてこれらの群はアーベル群であるから，すべての部分群は正規部分群である．ゆえに，$B_n(X)$ は $Z_n(X)$ の正規部分群である．したがって，剰余群を考えることができる．この剰余群は n **次元ホモロジー群**と呼ばれ，$H_n(X)$ で表わされる．これらのことをまとめておくと次のようである．

定義 9.4.4　X を上の条件を満たす単体複体とする．

(1) $C_n(X)$ は n **次元鎖群**であり，X の n 単体を基底とする自由アーベル群である．
(2) $\partial_n : C_n(X) \to C_{n-1}(X)$ は**境界作用素**であり，単体上の境界作用素を拡張して得られる準同型写像である．
(3) $Z_n(X)$ は n **次元輪体群**であり，境界準同型写像 $\partial_n : C_n(X) \to C_{n-1}(X)$ の核である．
(4) $B_n(X)$ は n **次元境界群**であり，境界準同型写像 ∂_{n+1} による $C_{n+1}(X)$ から $C_n(X)$ への像である．
(5) $H_n(X)$ は n **次元ホモロジー群**であり，これは $Z_n(X)/B_n(X)$ のことである．

境界だけ異なる $C_n(X)$ の 2 つの輪体は，すなわち，$B_n(X)$ による同じ剰余類に属している元は**ホモローグ**であると言われる．

これらの定義は空間の特別な三角形分割に依存しているように見える．すなわち，X が異なった単体的複体をもてば，それらのホモロジー群も異なっている可能性がある．次の重要な**不変性定理**は，このことは真ではないことを主張している．実際，そこには組み合わせ論的位相幾何学の方法の力がある．

定理 9.4.1　X を三角形分割可能な位相空間とする．この分割から決定されるホモロジー群は，他のいかなる三角形分割から決定されるホモロジー群とも同型である．

ホモロジーもまた位相的不変量であり，実際にホモトピー不変量である．任意の連続写像は単体上の写像を定義し，それはホモロジー群の間の準同型写像に拡張される．このことは，前節において基本群に対して見てきたことと似ている．この連続写像が同相写像ならば，得られる準同型写像は同型写像である．

定理 9.4.2　X, Y を三角形分割可能な位相空間とし，$h : X \to Y$ を連続写像とする．このとき，h はすべての n に対して，準同型写像 $h^* : H_n(X) \to H_n(Y)$ を引き起こす．h が同相写像ならば，h^* は同型写像である．さらに，X, Y がホモトープならば，それらのホモロジー群もまた同型写像である．

定理 9.4.1 の最後の叙述は，ホモトピーという概念はホモロジーという概念よりも強いことを主張している．すなわち，ホモトープな空間はホモロジーによっては区別されない．

9.5　ホモロジーの計算

代数学の基本定理に対する我々の最後の証明の基礎となる，一般の球のホモロジーとブラウアー次数を説明する前に，初等的なホモロジー計算のいくつかの例をあげよう．空間 X のホモロジーを求めるために，単体分割が必要である．定理 9.4.1 によって，この単体分割は任意のものでよい．しかし，このことは多くの場合かなり難しいので，ホモロジーの計算に役立つように様々な技術や定理が研究されてきた．例の中で用いるために，これらのいくつかを述べよう．

X が q 次元単体分割をもてば，すなわち，q より大きい次元の単体をもたない，とすれば，$n > q$ に対して $H_n(X) = 0$ が成り立つ．

次に，X が収縮可能な空間ならば，それは 1 点にホモトープである．ホモトピーはホモロジーを保存するから，収縮可能な空間のホモロジーは点 P のホモロジーと同じである．明らかに，$Z_0(P) = \mathbb{Z}$ である．一方，P は 0 次元であるから，$B_0(P) = 0$ である．したがって，$H_0(P) = \mathbb{Z}$ でかつ，$H_n(P) = 0$ $(n \geq 1)$ となる．

定理 9.5.1　X が収縮可能な空間ならば，$H_0(P) = \mathbb{Z}$ でかつ，$H_n(P) = 0$ $(n \geq 1)$ が成り立つ．

空間が連結でなければ，共通部分のない連結な部分の和集合に分割できる．これらは X の**連結成分**と呼ばれる．X が単体分割をもつと仮定する．このとき，これらの連結成分のそれぞれのなかで，任意の頂点は輪体である．さらに，$P_0, P_1, \ldots, P_t$ を 1 つの成分のなかの頂点とすれば，

$$P_k = P_0 + (P_1 - P_0) + \cdots + (P_k - P_{k-1}).$$

さて，各 $P_i - P_j$ は境界であるから $B_0(X)$ に属する．ゆえに，任意の頂点は $B_0(X)$ による同じ剰余類に属する．したがって，$H_0(X) = Z_0(X)/B_0(X)$ は

ちょうど1つの頂点を基底とする階数1の自由アーベル群である．任意の他の連結成分においても同じことが成り立つ．以上より，次の結果が得られた．

定理 9.5.2 X が n 個の連結成分をもつ単体的複体ならば，次が成り立つ．

$$H_0(X) = \text{階数 } n \text{ の自由アーベル群} \ \cong \mathbb{Z}^n.$$

最後に，次の定理を示すことができる．これは $\prod_1$ がわかっているとき，H_1 の計算を可能にするだけではなく，ホモロジーとホモトピーの間の関係も与える．G が群であるとき，そのアーベル化は $G^{ab} = G/G'$ であった (第 9.2 節参照). G がアーベル群ならば，$G^{ab} = G$ である．

定理 9.5.3 X が弧状連結である単体的複体ならば，次が成り立つ．

$$H_1(X) \cong \textstyle\prod_1(X)^{ab}.$$

$\prod_1(X)$ がアーベル群ならば，$H_1(X) \cong \prod_1(X)$.

例 9.5.1 円 S^1 のホモロジーを計算する．三角形分割は図 9.8 で与えられている．明らかに，S^1 のホモロジーは1つの三角形，すなわち，2単体の境界のホモロジーと同じである．

S^1 は連結であるから，それは1つの連結成分をもつので，$H_0(S^1) = \mathbb{Z}$ である．さらに，S^1 は1次元であるから，$H_n(S^1) = 0$ $(n > 1)$.

第 9.3 節で $\prod_1(S^1) = \mathbb{Z}$ であることを見た．これはアーベル群である．したがって，$H_1(S^1) \cong \prod_1(S^1) = \mathbb{Z}$ が成り立つ．この結果は三角形分割から直接得ることもできる．

$C_1(S^1)$ は P_0P_1, P_1P_2, P_2P_0 を基底とする自由アーベル群である．このとき，1 鎖は次の形をしている．

$$m_1P_0P_1 + m_2P_1P_2 + m_3P_2P_0 \quad (m_1, m_2, m_3 \in \mathbb{Z}).$$

境界をつくるときに，頂点 P_1 が消去されるただ1つの場合は $m_1 = -m_2$ のときだけである．同様に，P_2 が消去されるただ1つの場合は $m_3 = -m_2$ のときだけである．ゆえに，1 輪体は次の形でなければならない．

$$m(P_0P_1 - P_1P_2 + P_2P_0), \ (m \in \mathbb{Z}).$$

このことより，任意の輪体はただ 1 つの 1 鎖 $P_0P_1 - P_1P_2 + P_2P_0$ の倍数である．したがって，$Z_1(S^1) \cong \mathbb{Z}$ が成り立つ．2 鎖は存在しないから，$B_1(S^1) = 0$ である．よって，$H_1(S^1) = Z_1(S^1)/B_1(S^1) = \mathbb{Z}$ を得る．□

例 9.5.2 2 次元の球 S^2 を考える．S^1 を三角形のように三角形分割することができたように．図 9.11 に示すように，S^2 も四面体の表面のように三角形分割することができる．

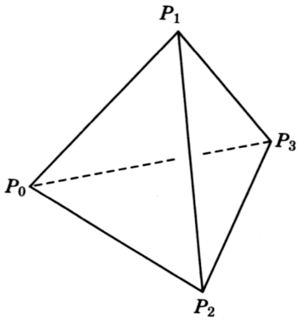


図 9.11　2 次元の球の三角形分割

さて，これは連結であるから，$H_0(S^2) = \mathbb{Z}$ である．明らかに，球の表面上のどんなループも 1 点に縮めることができるから，$\prod_1(S^2) = 0$ となる．そのとき，定理 9.5.3 より，$H_1(S^2) = 0$. これは 2 次元だから，$n > 2$ に対して $H_n(S^2) = 0$ となっている．次に $H_2(S^2)$ を考える．

2 鎖は次の形である．

$$m_1P_0P_1P_2 + m_2P_1P_2P_3 + m_3P_2P_3P_0 + m_4P_3P_0P_1 \quad (m_i \in \mathbb{Z}).$$

これが輪体ならば，面 $P_0P_1P_2, P_1P_2P_3$ の共通の辺は P_1P_2 であるが，これは消去されなければならない．このことは $m_2 = -m_1$ であることを意味している．他の面についての同一の推論によって，このとき輪体は次の形をしていることがわかる．

$$m(P_0P_1P_2 - P_1P_2P_3 + P_2P_3P_0 - P_3P_0P_1) \quad (m \in \mathbb{Z}).$$

すなわち，ただ 1 つの 2 鎖の倍数である．ゆえに，$Z_2(S^2) = \mathbb{Z}$ となる．S^2

は 2 次元であり，3 鎖は存在しないので $B_2(S^2)=0$. したがって，$H_2(S^2)=Z_2(S^2)/B_2(S^2)=\mathbb{Z}$ が得られる．

以上をまとめると，

$$\begin{aligned} H_0(S^2) &= \mathbb{Z}, \\ H_2(S^2) &= \mathbb{Z}, \\ H_n(S^2) &= 0 \quad (n \neq 0,2). \end{aligned}$$

□

例 9.5.3 トーラス T を考える．三角形分割は図 9.10 にある．T は連結であるから，$H_0(T)=\mathbb{Z}$. 群 $\prod_1(T)$ は階数 2 の自由アーベル群であるから，$H_1(T)\cong\prod_1(T)=\mathbb{Z}\times\mathbb{Z}$.

2 鎖は図 9.10 に描かれている 17 個の三角形 (2 単体) の和である．円に対する議論と球に対する議論におけるように，境界をとるとき，番号が 1,2 の三角形の共通の辺が消去されるただ 1 つ方法は，その係数が同じ大きさで符号が反対の場合である．これらの 2 単体を $T_1,\ldots,T_{17}$ で表せば，この議論より次のことがわかる．T における 2 輪体は $T_1-T_2+T_3-\cdots+T_{17}$ の倍数である．ゆえに，$Z_2(T)=\mathbb{Z}$ となっている．トーラスは 2 次元だから $B_2(T)=0$. したがって，$H_2(T)=\mathbb{Z}$ が成り立つ．

最後に，$n>2$ ならば $H_n(T)=0$ となる． □

例 9.5.4 X を 8 の形の図形，すなわち，図 9.6 においてすでに見た 2 つの円の花束とする．例 9.5.1 のように各円を三角形分割すれば，1 次元の単体的複体としてのこの図形の三角形分割を得る．

この図形は連結であるから，$H_0(X)=\mathbb{Z}$ である．$\prod_1(X)$ は階数 2 の自由群である (第 9.3 節参照). この群のアーベル化は階数 2 の自由アーベル群である．したがって，$H_1(X)=\prod_1(X)^{ab}=\mathbb{Z}\times\mathbb{Z}$ となる．最後に，$n>1$ に対して $H_n(X)=0$ $(n>1)$ が成り立つ． □

9.6　球のホモロジーとブラウアー次数

例 9.5.2 において，$n\geq 1, n\neq 2$ ならば $H_n(S^2)=0$ であり，$H_2(S^2)=\mathbb{Z}$ であることを見た．このことは，我々の代数学の基本定理の証明において重要である球の一般的な性質である．n 次元球とは

$$S^n=\{(x_0,\ldots,x_n)\in\mathbb{R}^{n+1}\,;\,x_0^2+\cdots+x_n^2=1\}$$

に同相な集合であることを思い出そう．一般に，n 次元球は $(n+1)$ 単体の表面に同相である．したがって，1 次元球 S^1 は三角形に同相であり，2 次元球 S^2 は四面体の表面に同相である，等々．例 9.5.1 と例 9.5.2 において用いられた議論を拡張し精密化すれば，次の定理が証明される．

定理 9.6.1　$n \geq 1$ として，S^n を n 次元球とする．このとき，$H_0(S^n) = \mathbb{Z}$ であり，$q \geq 1$ に対して，

$$\begin{aligned} H_n(S^n) &= \mathbb{Z}, \\ H_q(S^n) &= 0 \quad (n \neq q). \end{aligned}$$

さて，S^n, Σ^n を n 次元球として，連続写像 $f : S^n \to \Sigma^n$ を考える．これは準同型写像 $f^* : H_n(S^n) \to H_n(\Sigma^n)$ を引き起こす．定理 9.6.1 によって，$H_n(S^n)$ は無限巡回群である．α を $H_n(S^n)$ の生成元とする．同様に，$H_n(\Sigma^n)$ は無限巡回群であり，β をその生成元とする．f^* は準同型写像であるから，$f^*(\alpha)$ は β の整数倍である．すなわち，適当な整数 m が存在して

$$f^*(\alpha) = m\beta$$

と表される．整数 m は写像 f の**ブラウアー次数**，あるいは**写像度**と呼ばれる．これを，簡単に $\deg(f)$ と表す．直感的に，$\deg(f)$ は像 $f(S^n)$ が Σ^n のまわりをまわる回数を表している代数的な数である．

次の次数に関する 3 つの結果は，代数学の基本定理の証明において重要である．証明は長いので割愛する．

補題 9.6.1　連続写像の写像度は S^n と Σ^n の単体分割の仕方には無関係である．

この補題は必要である．なぜならば，$H_n(S^n)$ と $H_n(\Sigma^n)$ が 2 つとも無限巡回群であったとしても，$H_n(S^n)$ を生成している輪体 α への f の作用は異なった三角形分割に対しては違ってくる可能性がある．この補題は，ある球から他の球へ写像するときに，ホモロジーの違いを除いてこのようなことは起こらないということを主張している．

補題 9.6.2

(1) n 次元球 S^n から n 次元球 Σ^n への連続写像 f の写像度は，f のホモトピー類にのみ依存する．特に，2 つのホモトープな写像 $f : S^n \to \Sigma^n$, $g : S^n \to \Sigma^n$ は同じ写像度をもつ．

(2) $f : S^n \to \Sigma^n, g : S^n \to \Sigma^n$ が $\deg(f) = \deg(g)$ を満たす 2 つの連続写像とすれば，f と g はホモトープである．

この補題は，ホモトピーを除いて完全に n 次元球の間の連続写像を分類する．特に，ホモトピー類は整数の集合と 1 対 1 に対応する．

定理 9.6.2 $f : S^n \to \Sigma^n$ で $\deg(f) \neq 0$ ならば，Σ^n の任意の点は像 $f(S^n)$ の中にある．

この定理は我々の最後の証明において重要な手段となる．

この節を閉じるにあたって，ブラウアーによる有名な結果「**ブラウアーの不動点定理**」を述べておこう．この定理はブラウアー次数を用いて証明される．$f : X \to Y$ とする．$x_0 \in X$ が $f(x_0) = x_0$ を満たすとき，点 x_0 は f に関する**不動点**という．

定理 9.6.3（ブラウアーの不動点定理）D^n を単位 n 次元球体とする．すなわち，単位球 $S^{n-1} \subset \mathbb{R}^n$ の内部および境界とし，$f : D^n \to D^n$ を連続写像とする．このとき，f は少なくとも 1 つの不動点をもつ．

9.7 代数学の基本定理——証明 6

ここで，我々の最終の証明を与えよう．図 9.12 のように原点 $(0,0,0)$ において複素平面に接している単位球 S^2 を考える．

この球を次のようなやり方で $\mathbb{C}$ 上に写像する．$N = (0,0,1)$ を北極とし，$w \in S^2 - N$ に対して w と N を結んだ直線をつくる．この直線は平面 $\mathbb{C}$ とただ 1 つの点 $p(w)$ で交わる．この写像は**立体射影**と呼ばれる．この写像に対する方程式は明確に表現されるが（文献 [A] 参照），我々が必要なのは p は $\mathbb{C}$ と $S^2 - N$ の間の連続的な全単射であるという事実である．北極と ∞ とを同一視すれば p は S^2 から $\mathbb{C} \cup \infty$ への全単射である．写像 p は等角写像であ

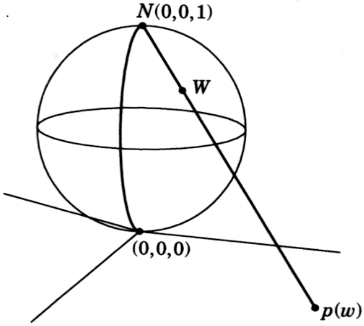


図 **9.12**　立体的な射影

ることが示され，したがって，S^2 は拡張された複素平面 $\mathbb{C}\cup\infty$ の等角モデルを与える．このような仕方で S^2 を見るとき，それは**リーマン球面**と呼ばれる．

定理 9.7.1　立体射影 p は S^2 と $\mathbb{C}\cup\infty$ の間の等角な全単射を与える．

さて，$P(z)=a_0+a_1z+\cdots+a_nz^n$ $(a_n\neq 0)$ を定数でない次数 n の複素多項式とする．$P(z)$ の根を求めようとしており，$a_n\neq 0$ であるから，一般性を失わずに $a_n=1$ と仮定してよい．したがって，$P(z)=a_0+a_1z+\cdots+z^n, n>1$ を考えよう．$P(\infty)=\infty$ であるから，$P(z)$ はリーマン球面をリーマン球面に写像していると考えることができる．すなわち，$P(z)$ は連続写像 $S^2\to S^2$ である．このようにして，それはブラウアー次数 m をもつ．まずはじめに，そのブラウアー次数はその多項式 $P(z)$ の次数と同じであることを示す．

補題 9.7.1　$P(z)$ は写像 $f(z)=z^n$ とホモトープである．

(証明)　$t\in[0,1]=I$ とする．$z\in\mathbb{C}$ に対して，$H(z,t)=z^n+(1-t)(a_0+a_1z+\cdots+a_{n-1}z^{n-1})$ とし，$z=\infty$ のとき，$H(\infty,t)=\infty$ とする．明らかに，$H(z,t)$ は $\mathbb{C}\times I\to\mathbb{C}$ なる連続写像である．ここで，すべての $t\in[0,1]$ に対して $\lim_{z\to\infty}H(z,t)=\infty=H(\infty,t)$ であるから，$H(z,t)$ は 連続写像 $(\mathbb{C}\cup\infty)\times I\to\mathbb{C}\cup\infty$ である．したがって，$H(z,t)$ は 連続写像 $S^2\times I\to S^2$ である．$H(z,0)=P(z)$ かつ $H(z,1)=z^n$ であるから，これは 1 つのホモトピーを定義する．　■

補題 9.7.2 $f(z)=z^n$ のブラウアー次数は n である．したがって，複素多項式に対して，ブラウアー次数と多項式の次数は一致する．

（**証明**）図 9.13 に描かれているように，$S^2(\mathbb{C}\cup\infty$ と考えられている$)$ の 2 つの三角形分割を考える．

$f(z)=z^n$ によって，図 (A) の n 個の影のついた部分は，向きを保存する仕方で図 (B) の 1 つの影のついた部分の上に写像される．写像は三角形分割 (A) における輪体を三角形分割 (B) における輪体に n 回写像する．したがって，z^n の次数は n である． ■

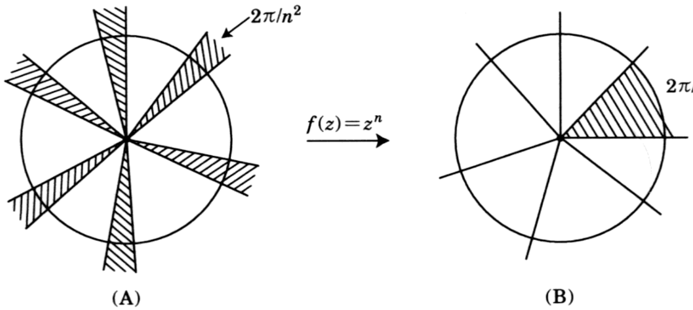


図 **9.13** $f(z)=z^n$ の回転数

定理 9.7.2（代数学の基本定理）$P(z)$ を定数でない複素多項式とする．このとき，$P(z)$ は 1 つの複素数の根をもつ．

（**証明**）$P(z)=a_0+a_1z+\cdots+a_nz^n$ とする．$P(z)$ は定数でないと仮定しているから，$n>0$ でかつ $a_n\neq 0$ としてよい．ゆえに，上で見たように $a_n=1$ と仮定できる．補題 9.7.1 より，$P(z)$ は $f(z)=z^n$ にホモトープである．補題 9.7.2 と補題 9.6.2 より，$P(z)$ はブラウアー次数 $n\neq 0$ をもつ．定理 9.6.2 より，S^2 の任意の点は $P(z)$ の像の中にある．特に，$P(z_0)=0$ を満たす少なくとも 1 つの点 $z_0\in S^2$ が存在する．$P(\infty)=\infty$ であるから，$z_0\in\mathbb{C}$ であることがわかる． ■

9.8　結論

これで，本書が目指していた 3 つの方向からの代数学の基本定理の証明の最後のもの，すなわち，位相的な証明が完成した．位相的な状況においては，第 8.1 節において与えられた直接的な証明とこの節において与えられた最後の証明は 2 つとも回転数を用いていたということに注意しよう．また，代数学の基本定理の証明にとって，実際一般のブラウアー次数についてのすべてを必要としない．ただ，2 次元球に対するブラウアー次数だけが必要であったということにも注意しよう．

付録 D において，この本のテーマとは若干違ったかたちの，位相的に動機づけられた 2 つの証明を呈示しよう．

演習問題

9.1　H と K を群として，それらの直積 $H \times K$ もまた $(h,k)(h_1,k_1) = (hh_1,kk_1)$ という演算によって群であることを証明せよ．

9.2　補題 9.2.1 を証明せよ．

9.3　補題 9.2.2 を証明せよ．

9.4　p,q を互いに素である素数とするとき，$\mathbb{Z}_p \times \mathbb{Z}_q$ は巡回群であることを証明せよ．これは巡回群の直積は巡回群になることもある，ということを示している．

9.5　$\mathbb{Z}_2 \times \mathbb{Z}_2$ は巡回群ではないことを示せ．これは巡回群の直積は必ずしも巡回群ではないということを示している．

9.6　すべての有限生成アーベル群は巡回群の直積であることを証明せよ (ヒント：2 つの生成元に対して，これを示せ)．

9.7　有限アーベル群は可換 p 群の直積であることを証明せよ (ヒント：G において，G の位数の約数である素数 p に対して，p のベキを位数とするすべての元の集合は部分群であることを示せ．このとき，G の位数のすべての約数に対して，この形のすべての部分群を考えると，G はこれらの部分群の直積となることを示せ)．

9.8　次の位数をもつすべての有限アーベル群を完全に分類せよ．

(i) 25，(ii) 45，(iii) 37，(iv) 1284．

9.9　X と Y が同相空間であれば，それらはホモトープであることを証明せよ．

9.10　すべての収縮可能な空間はホモトープであることを証明せよ．

9.11　n 個の円の花束の基本群の一般的な元を書き表せ．

9.12　$\prod_1(X) = \mathbb{Z}_2 \times \mathbb{Z}_2$ とする．ホモトピーを除いて，X の被覆空間はいくつあるか．

9.13　n 個の円の花束のホモロジーを決定せよ．

9.14　$P_0P_1P_2P_3$ を 3 単体とすれば，$\partial_2\partial_3(P_0P_1P_2P_3) = 0$ が成り立つことを証明せよ．

9.15　2 つの接している 2 次元球のホモロジーを計算せよ．

付録A

ガウスのオリジナルの証明

代数学の基本定理のガウスによる最初の証明は，我々がここまで見てきた6個の証明のどれとも本質的に異なっている．この最初の証明は1799年に彼の学位論文において与えられたものであり，1849年に発表された第4の証明は最初のものとは別のかたちをとっている．この節においては，ガウスのオリジナルの証明の比較的現代的なバージョンを与える．この証明はUpsensky[U]の本から必要なことを適宜引用している．

定数でない複素多項式

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

を考える．これまでと同様に，最高次数の係数は1でかつ定数項 a_0 は0でないと仮定してよい．さらに， $n > 2$ と仮定できる． $n = 1$ のときは単なる1次方程式であるから，明らかに1つの根をもつ． $n = 2$ のときは2次方程式の根の公式より，複素数の根をもつことがわかる． $n > 2$ として，その係数は次のような極形式で与えられていると仮定する．

$$a_{n-1} = A(\cos\alpha + i\sin\alpha), a_{n-2} = B(\cos\beta + i\sin\beta), \ldots, a_0 = L(\cos\lambda + i\sin\lambda).$$

また，変数は $z = r(\cos\phi + i\sin\phi)$ とする．多項式は実部と虚部にわけて次のように表すことができる(第4章を参照)．

$$f(z) = T(z) + iU(z). \tag{A.1}$$

ド・モアブルの定理と係数の極座標表示を使えば，T と U は r と ϕ によって次のように表される．

$$T = r^n \cos n\phi + Ar^{n-1}\cos((n-1)\phi + \alpha) + \cdots + L\cos\lambda, \tag{A.2}$$

$$U = r^n \sin n\phi + Ar^{n-1}\sin((n-1)\phi + \alpha) + \cdots + L\sin\lambda, \tag{A.3}$$

代数学の基本定理の証明のために，$T(z_0), U(z_0)$ が同時に 0 である点 z_0 が存在することを証明しなければならない．

まず最初に，$r > R$ に対して

$$r^n - \sqrt{2}(Ar^{n-1} + Br^{r-2} + \cdots + L) > 0 \tag{A.4}$$

を満たす実数 R を求めることが可能である．これを見るために，S をすべての $A, B, \ldots, L$ より大きい実数の定数とする．このとき，$R = 1 + \sqrt{2}S$ とおく．$r > R$ ならば，$r > 1 + \sqrt{2}S$ であるから $1 - \dfrac{\sqrt{2}S}{r-1} > 0$ である．$r > R > 1$ より，$\dfrac{1}{r} + \dfrac{1}{r^2} + \cdots + \dfrac{1}{r^n} < \dfrac{1}{r-1}$ が成り立つ．したがって，

$$r^n \left(1 - \sqrt{2}S(\frac{1}{r} + \frac{1}{r^2} + \cdots + \frac{1}{r^n})\right) > 0.$$

ゆえに，

$$r^n - \sqrt{2}S(r^{n-1} + \cdots + 1) > 0.$$

よって，

$$r^n - \sqrt{2}(Ar^{n-1} + Br^{n-2} + \cdots + L) > 0.$$

次に，半径 $r > R$ の円の円周は $2n$ 個の円弧から構成されている．その円弧上の内側では，図 A.1 におけるように T は交代に正負の値をとる．

このことを見るために，$\theta = 4\pi/n$ とおき，半径 $r > R$ の円上でそれぞれ $\theta, 3\theta, \ldots, (8n-3)\theta, (8n-1)\theta$ を偏角とする $4n$ 個の点 $P_0, P_1, \ldots, P_{4n-1}$ を考える．

P_{2k} と P_{2k+1} に対応する偏角は　$\phi = (4k+1)\dfrac{\pi}{4n}$ と　$\phi' = (4k+2)\dfrac{\pi}{4n}$ である．したがって，

$$\cos(n\phi) = (-1)^k \frac{1}{\sqrt{2}}, \quad \cos(n\phi') = (-1)^{k+1}\frac{1}{\sqrt{2}}.$$

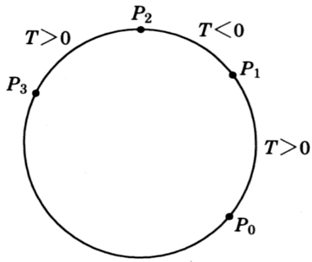


図 A.1　半径 r の円上の T

T の対応している値に $(-1)^k$ と $(-1)^{k+1}$ をかけると，それぞれ次のようになる．

$$\begin{aligned}(-1)^k T &= \frac{r^n}{\sqrt{2}} + (-1)^k A r^{n-1}\cos((n-1)\phi+\alpha) + \cdots + (-1)^k L\cos\lambda,\\ (-1)^{k+1} T &= \frac{r^n}{\sqrt{2}} + (-1)^{k+1} A r^{n-1}\cos((n-1)\phi'+\alpha)\\ &\quad + \cdots + (-1)^{k+1} L\cos\lambda.\end{aligned}$$

$(-1)^k\cos((n-1)\phi+\alpha),\ldots,(-1)^k\cos\lambda$, また，$(-1)^{k+1}\cos((n-1)\phi'+\alpha),\ldots,(-1)^{k+1}\cos\lambda$ を (-1) によって置き換えれば，次の不等式を得る．

$$\begin{aligned}(-1)^k T &\ge \frac{r^n}{\sqrt{2}} - AR^{n-1} - \cdots - L,\\ (-1)^{k+1} T &\ge \frac{r^n}{\sqrt{2}} - AR^{n-1} - \cdots - L.\end{aligned}$$

これら 2 つの不等式の右辺は R の選び方により正であるので，主張が示されたことになる．

さて，T は ϕ と共に連続的に変化するので，それはその円上で少なくとも $2n$ 回 0 になる．$2n$ 個の点 $Q_0, Q_1, \ldots, Q_{2n-1}$ で 0 になると仮定し，それらの偏角をそれぞれ　θ, 3θ, 5θ, $7\theta,\ldots,(8n-3)\theta$, $(8n-1)\theta$ とする．$\zeta=\tan(\phi/2)$ とおけば

$$\cos\phi = \frac{1-\zeta^2}{1+\zeta^2},\quad \sin\phi = \frac{2\zeta}{1+\zeta^2}$$

となっている．そこで，$z = r\dfrac{1-\zeta^2}{1+\zeta^2} + i\dfrac{2\zeta}{1+\zeta^2}$ とおく．ここで，もとの多項式 $f(z)$ を考えると，その実部は次のようになる．

$$T = \frac{p_{2n}(\zeta)}{(1+\zeta^2)^n}.$$

ここで，$p_{2n}(\zeta)$ は次数が $2n$ 以下の実多項式である．この多項式は $2n$ 個の零点をもつので，次数はちょうど $2n$ であり他の根をもたない．したがって，この円周上で T がゼロになる点は　$Q_0, Q_1, \ldots, Q_{2n-1}$ だけである．ゆえに，T の値は図 A.1 のようにこの円上で交互に正負の値をとる．

第 3 に，虚部 U は $Q_0, Q_2, \ldots, Q_{2n-2}$ において正の値をとり，$Q_1, Q_3, \ldots,$ Q_{2n-1} において負の値をとる．Q_k の偏角　ϕ は $(4k+1)\pi/4n$ と $(4k+3)\,\pi/4n$ の間になる．ゆえに，$(-1)^k \sin(n\phi) \geq 1/\sqrt{2}$ となる．U に $(-1)^k$ をかけて，$(-1)^k \sin((n-1)\phi+\alpha), \ldots, (-1)^k \sin\lambda$ を -1 で置き換えると次の不等式が成り立つ．

$$(-1)^k U \geq r^n (-1)^k \sin(n\phi) - AR^{n-1} - \cdots - L.$$

したがって，次の不等式を得る.,

$$(-1)^k U \geq \frac{r^n}{\sqrt{2}} - AR^{n-1} - \cdots - L.$$

右辺は R の選び方より正であるから，Q_k における U の符号は $(-1)^k$ である．

半径 $r > R$ の円 Γ を考える．その円周は点 $Q_0, Q_1, \ldots, Q_{2n-1}$ によって，交互に T の符号が変わる $2n$ 個の円弧に分けられる．円 Γ の半径を大きくするとき，円弧 $Q_0Q_1, Q_1Q_2, \ldots$ はその上で T の値が交互に正負となる $2n$ 個の無限大に広がっている集合を定める．そして，これらの集合は $T=0$ によって定まる曲線によって分離されている．ガウスと Upsensky の研究から借用して，$T>0$ である Γ の外側の集合を**海**，$T<0$ であるの集合を**陸**と呼ぶ．$T=0$ である曲線を**海岸線**と呼ぶ．n 個の海と n 個の陸はそれら自身様々に円弧を横切って Γ の内部に広がっている．Q_1 から出発して，海岸線に沿って陸が常に右内側にあるように動く．最期に Γ を出なければならない．再びそれを横切るとき，陸地はなお右側になければばらない．円周が反時計回りにまわるとすれば，陸地と海は交互に現れる．したがって，偶数点 Q_{2k}, すなわち，$Q_2, Q_4, \ldots$ において外側に向けて出なければならない．このようにして，Q_1 からある点 Q_{2k} へいたる連続な道 γ が存在する．道 γ 上では $T=0$ である．Q_1 で $U<0$, ところが Q_{2k} では $U>0$ である．U は道 γ に沿って，連続な関数であるから，γ 上のある点において 0 という値をとる．この点において，T, U は両方とも 0 となる．このことは，$f(z)$ の根の存在を示している．

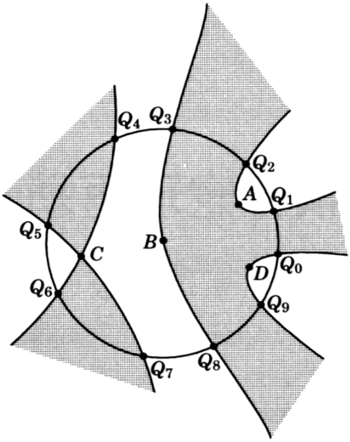


図 A.2　ある 5 次の多項式の陸地と海

図 A.2 はガウスによって研究された次数が 5 の特別な多項式に対して，以上述べたことを表している．Q_1 から出発して，海岸線に沿って Q_2 に行く．Q_1 において $U<0$ であり，一方 Q_2 においては $U>0$ である．海岸線に沿って $T=0$ であるから，$U=0$ である点，すなわち図の中で A という記号で表されている点が存在しなければならない．この点が根を表している．同様に，点 B,C,D も根を表している．C 点は重根であり，他のものは単根である．

付録B

コーシーの積分定理再訪

第 5 章で，複素解析学のリウヴィルの定理に基づいた代数学の基本定理の第 2 の証明を与えた．そして，リウヴィルの定理は，$f(z)$ がある領域 U で解析的ならば，U において連続的に微分可能な任意の閉曲線 γ に対して $\displaystyle\int_\gamma f(z)dz = 0$ が成り立つ，というコーシーの積分定理に基づいていた．そのときには，$f'(z)$ が連続であるという事実に基づいているグリーンの定理を使う証明を与えた．これはコーシーのオリジナルの証明であった．しかしながら，我々は前にグールサはこの条件を除いたことに言及しておいた．この節では，この重要な定理に立ちもどり，星状領域に対してコーシー・グールサの定理の証明を与えよう．付録 C において，ここで発展させた概念のいくつかを用いて，代数学の基本定理のさらに 3 つの複素解析的な証明を与えるつもりである．

$\mathbb{C}$ の領域 U は，任意の 2 点 $z_1, z_2 \in U$ が U に完全に含まれている曲線によって結ばれているとき，**弧状連結**であるという．さらに，開集合が弧状連結であるための必要十分条件は任意の 2 点 $z_1, z_2 \in U$ に対して，z_1 と z_2 を結ぶ**多角形的曲線**が存在することである．(多角形的曲線とは，有限個の線分からなる曲線のことである．開集合の場合にはこの多角形的曲線は，その各線分が座標軸に平行になるようにとることができる．)

線積分の概念を少し拡張しなければならない．U を $\mathbb{C}$ の集合とし，$\gamma_i : [a_i, b_i] \to U \subset \mathbb{C}$, $(a_i \le b_i, i = 1, 2)$ を U の 2 つの曲線で $\gamma_1(b_1) = \gamma_2(a_2)$ を

満たしているものとする．このとき，U における**和** $\gamma = \gamma_1 + \gamma_2$ を

$$\gamma : [a_1, b_2 - a_2 + b_1] \to U$$

によって定義する．ここで，

$$\begin{aligned} \gamma(t) &= \gamma_1(t), & t \in [a_1, b_1], \\ \gamma(t) &= \gamma_2(t + a_2 - b_1), & t \in [b_1, b_2 - a_2 + b_1]. \end{aligned}$$

同様にして，U における有限個の曲線の和 $\gamma_1 + \gamma_2 + \cdots + \gamma_m$ を定義することができる．この曲線の和は結合的である．

曲線 $\gamma : [a, b] \to \mathbb{C}$ $(a \leq b)$ は，有限個の連続的微分可能な曲線 $\gamma_1, \ldots, \gamma_m$ が存在して，$\gamma = \gamma_1 + \cdots + \gamma_m$ を満たすとき，**区分的に連続的微分可能**と呼ばれる．このことは，次のように言うことができる．$a = a_1 < a_2 < \ldots < a_{m+1} = b$ を満たす点 $a_1, \ldots, a_{m+1}$ が存在して，γ_i は各区間 $[a_i, a_{i+1}]$ $(1 \leq i \leq m)$ を定義域とする連続的微分可能な曲線になっている．たとえば，任意の多角形的曲線は部分的に連続的微分可能である．

U を $\mathbb{C}$ の開集合とし，曲線 $\gamma : [a, b] \to \mathbb{C}$ $(a \leq b)$ を有限個の連続的微分可能な曲線 $\gamma_1, \ldots, \gamma_m$ の和 $\gamma = \gamma_1 + \cdots + \gamma_m$ とする．$f : U \to \mathbb{C}$ を連続関数とする．このとき，線積分を次のように定義する．

$$\int_\gamma f(z)dz = \sum_{i=1}^{m} \int_{\gamma_i} f(z)dz.$$

上の曲線 $\gamma = \gamma_1 + \cdots + \gamma_m$ の弧の長さは $L(\gamma) = L(\gamma_1) + \cdots + L(\gamma_m)$ によって定義される．ここで，$L(\gamma_i)$ は第 5 章で定義したように

$$L(\gamma_i) = \int_{\gamma_i} |dz| \quad (i = 1, \ldots, m)$$

である．γ 上で $|f(z)| \leq M$ ならば，補題 5.2.1 と定義より次が成り立つ．

$$\left| \int_\gamma f(z)dz \right| \leq ML(\gamma).$$

以下，付録 B の残りと付録 C において，曲線は常に上で定義した区分的に連続的微分可能であると仮定する．

定義 B.1 部分集合 $M \subset \mathbb{C}$ は，ある点 $z_1 \in M$ が存在して，任意の点 $z \in M$ に対して線分 $\overline{z_1 z}$ が M に含まれるとき，**星状**であるという．z_1 は M の**中心**と呼ばれる．明らかに，星状集合は弧状連結である．

$U \subset \mathbb{C}$ が開集合でかつ星状集合であるとき，**星状領域**という．

例 B.1 次の集合はすべて星状領域である．

(a) $\mathbb{C}$ または $\mathbb{R}$ は 0 を中心とする星状領域である．

(b) 任意の円の内部は星状領域である．

(c) $H = \{z\,;\, Im(z) > 0\}$ は i を中心とする星状領域である．

(d) $\mathbb{C}^- = \{z \in \mathbb{C};\, z \notin \mathbb{R}$ または $z \in \mathbb{R}, z > 0\}$.

定義 B.2 $U \subset \mathbb{C}$ を開集合で，$f : U \to \mathbb{C}$ を連続関数とする．解析関数 $F : U \to \mathbb{C}$ が $F' = f$ を満たすとき，F は U における f の**原始関数**という．

第 5 章と上の定義から，F が U における f の原始関数ならば，次が成り立つ．

$$\int_\gamma f(z)dz = \int_\gamma F'(z)dz = F(\gamma(t_1)) - F(\gamma(t_0)).$$

ただし，$\gamma(t_1), \gamma(t_0)$ は曲線 γ 上の端点である．ゆえに，連続関数が U において原始関数をもてば，それはコーシーの積分定理を満足する．グールサの証明は，本質的に星状領域における任意の解析関数は原始関数をもつことを示すことから成り立っている．はじめに，原始関数の存在に対して積分可能性を結びつけなければならない．

定義 B.3 $U \subset \mathbb{C}$ を開集合とする．関数 $f : U \to \mathbb{C}$ は U において連続であり，かつ U において原始関数をもつとき，U において**積分可能**であるという．

定理 B.1（積分可能判定条件）$U \subset \mathbb{C}$ を領域とする．関数 $f : U \to \mathbb{C}$ は U において連続であると仮定する．このとき，次の条件は同値である．

(1) f は U で積分可能である．

(2) U の任意の曲線 γ に対して，$\displaystyle\int_\gamma f(z)dz = 0$ が成り立つ．

(2) が成り立つとき，点 $z_1 \in U$ を固定し，任意の点 $z \in U$ に対して z_1 から z への曲線 γ を選ぶ.

$$F(z) = \int_\gamma f(z)dz,\ z \in U$$

と定義すると，$F(z)$ は U において $f(z)$ の原始関数である.

（証明） (1) ならば (2) であることは明らかなので，(2) ならば (1) であることを証明すればよい．さらに，上の定理のなかで定義された $F(z)$ が $f(z)$ の原始関数であることを示せば十分である．したがって，すべての $z \in U$ に対して $F'(z) = f(z)$ を示す.

U の任意の閉曲線に対して，$\int_\gamma f(z)dz = 0$ であるから，関数 $F(z)$ は矛盾なく定義される (定理 5.2.2 参照)．そのとき，証明は定理 5.2.2 のそれと同じである.

$$\begin{aligned} F'(z) &= \lim_{\Delta z \to 0} \frac{F(z+\Delta z) - F(z)}{\Delta z} \\ &= \lim_{\Delta z \to 0} \frac{1}{\Delta z}\left(\int_{z_0}^{z+\Delta z} f(w)dw - \int_{z_0}^{z} f(w)dw\right) \\ &= \lim_{\Delta z \to 0} \frac{1}{\Delta z} \int_{z}^{z+\Delta z} f(w)dw. \end{aligned}$$

$f(z)$ は連続であるから，次のことを示すことができる (第 5 章の演習問題参照).

$$\int_z^{z+\Delta z} f(w)dw = (f(z) + \epsilon)(\Delta z),$$

ここで，$\Delta z \to 0$ のとき $\epsilon \to 0$ である.

したがって，

$$\lim_{\Delta z \to 0} \int_z^{z+\Delta z} f(w)dw = f(z).$$

よって，$F'(z) = f(z)$ を得る.　■

次に，星状領域 U における $f(z)$ の積分可能性は U の任意の三角形 $\triangle$ の境界に対して，$\int_{\partial\triangle} f(z)dz = 0$ が成り立つという事実から導かれることを示そう.

定理 B.2（積分可能性に対する三角形判定法）U を z_0 を中心とする星状領域とし，$f: U \to \mathbb{C}$ を連続とする．z_0 を頂点とする任意の三角形 $\triangle \subset U$ の境界 $\partial\triangle$ に対して

$$\int_{\partial\triangle} f(z)dz = 0$$

が成り立つならば，$f(z)$ は U において積分可能である．さらに，関数

$$F(z) = \int_{\overline{z_0 z}} f(z)dz$$

は U において $f(z)$ の原始関数である．特に，U における任意の閉曲線 γ に対して $\displaystyle\int_\gamma f(z) = 0$ が成り立つ．

（証明） U の任意の z に対して $\overline{z_o z} \subset U$ であるから，$F(z)$ は矛盾なく定義される．$c \in U$ を固定し，$z \in U$ を頂点 z_0, z, c とする三角形 $\triangle$ が U に含まれるように選ぶ．図 B.1 においてこれを図示する．

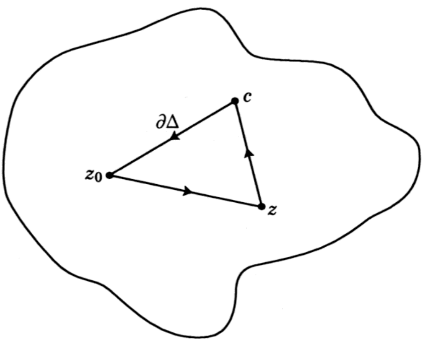


図 B.1　三角形判定条件

$\displaystyle\int_{\partial\triangle} f(z)dz = 0$ であるから，次が成り立つ．

$$F(z) = F(c) + \int_{\overline{cz}} f(w)dw.$$

このとき，定理 5.2.2 と定理 B.1 の証明のようにして，$F(z)$ は $F'(c) = f(c)$ $(c \in U)$ を満たす微分可能な複素関数であることがわかる．■

ここで，拡張されたコーシーの積分定理のグールサによる証明のなかで，重要な役割を果たす判定条件を与える．

定理 B.3（グールサの積分補助定理）$U \subset \mathbb{C}$ を開集合とし，$f : U \to \mathbb{C}$ を解析関数とする．$\triangle \subset U$ を三角形とするとき，次が成り立つ．

$$\int_{\partial\triangle} f(z)dz = 0.$$

（証明） 最初に，2 つの初等幾何学的事実を述べる．$\triangle$ を任意の三角形とし，L は長さを表すものとする．このとき，次が成り立つ．

(1) $\mathrm{Max}_{w,z\in\triangle}|w-z| \leq L(\partial\triangle)$.

(2) $\triangle$ の辺の中点を結んだ線分をひくことによって得られる 4 つの合同な部分三角形 $\triangle'$ の 1 つに対して $L(\partial\triangle') = \dfrac{1}{2}L(\partial\triangle)$ が成り立つ．これらの部分三角形については図 B.2 を参照せよ．

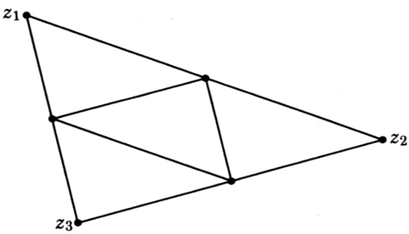


図 B.2　合同な部分三角形

$v(z) = \int_{\partial\triangle} f(z)dz$ と定義する．図 B.2 のように，4 つの合同な部分三角形 $\triangle_v$ $(v = 1, 2, 3, 4)$ が得られるように $\triangle$ の辺の中点を結んだ線分をひく．そのとき，中点を結んだ線分上の積分は異なる符号をもって 2 回現れるので，打ち消しあって消える．ゆえに，

$$v(z) = \sum_{v=1}^{4} \int_{\partial\triangle} f(z)dz = \sum_{v=1}^{4} v(\triangle_v)$$

が成り立つ．これを図 B.3 で示す．

4 つの積分から，最大の絶対値をもつものを 1 つ選び，この選ばれた積分に対する三角形を $\triangle^1$ とする．このとき，

$$|v(\triangle)| \leq 4|v(\triangle^1)|.$$

同じ分割と選び方を適用して，第 2 の部分三角形 $\triangle^2$ を得る．このとき，

$$|v(\triangle)| \leq 4|v(\triangle^1)| \leq 4^2|v(\triangle^2)|.$$

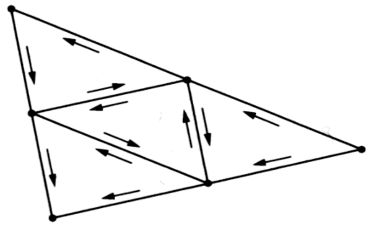


図 B.3　合同な部分三角形

この操作を続けると，有界閉集合である三角形の減少列

$$\triangle^1 \supset \triangle^2 \supset \cdots \supset \triangle^n \supset \cdots$$

が得られ，

$$|v(\triangle)| \leq 4^n |v(\triangle^n)|, (n = 1, 2, \dots)$$

が成り立っている．証明の最初になされた初等幾何学的注意の (2) より，

$$L(\partial\triangle^n) = \frac{1}{2^n} L(\partial\triangle),\ (n = 1, 2, \dots).$$

$\mathbb{R}^2$ における集積した図形の性質より，共通集合 $\bigcap_{n=1}^{\infty} \triangle^n$ はただ 1 つの点 $c \in \triangle$ を含む．$f(z)$ は解析関数であるから，

$$f(z) = f(c) + f'(c)(z - c) + (z - c)g(z),\ z \in U,\ g(c) = 0$$

を満たす連続関数 $g : U \to \mathbb{C}$ が存在する．原始関数の存在より，

$$\int_{\partial\triangle^n} f(c)dz = 0, \quad \int_{\partial\triangle^n} f'(c)(z - c)dz = 0,\ (n \geq 1)$$

が成り立つ．ゆえに，

$$v(\triangle^n) = \int_{\partial\triangle^n} (z - c)g(z)dz,\ (n \geq 1).$$

これより，

$$v(\triangle^n) \leq \max_{z \in \partial\triangle^n} (|z - c||g(z)|) L(\partial\triangle^n).$$

今度は初等幾何学的注意の (1) によって，この不等式より次を得る．

$$v(\triangle^n) \leq (L(\partial\triangle^n))^2 \max_{z \in \partial\triangle^n} |g(z)|\ \ (n = 1, 2, \dots).$$

前のとあわせて考えると

$$|v(\triangle)| \leq 4^n|v(\triangle^n)| \leq L(\partial\triangle)^2 \max_{z\in\partial\triangle^n} |g(z)| \ (n = 1, 2, \ldots).$$

$g(c) = 0$ でかつ $g(z)$ は c で連続であるから，任意の $\epsilon > 0$ に対して，ある $\delta > 0$ が存在して，c を中心とする半径 δ の球 $B_\delta(c)$ 上で $|g(z)| \leq \epsilon$ を満たしている．この δ に対して，正の整数 n_0 が存在して $n \geq n_0$ に対して $\triangle^n \subset B_\delta(c)$ が成り立つ．ゆえに，すべての $n \geq n_0$ に対して，Δ^n の境界上で $|g(z)| \leq \epsilon$ となるので，

$$|v(\triangle)| \leq (L(\partial\triangle))^2\epsilon.$$

$L(\partial\triangle)$ は固定されており，$\epsilon > 0$ は任意であるから，$v(\triangle) = 0$ が得られ，したがって，定理が証明された．■

さて我々は今星状領域に対する一般のコーシーの積分定理を証明した．これは第 5 章において述べたものと本質的に同じものである．しかしながら，そこで輪郭を示した証明において，その導関数 $f'(z)$ は連続であると仮定しているグリーンの定理を用いていた．この仮定は常に必要であった．ところが，それは単に $f(z)$ が解析的であるということを仮定している一般のコーシー・グールサの定理の 1 つの帰結である．

定理 B.4（星状領域に対するコーシー・グールサの定理）$U \subset \mathbb{C}$ を z_0 を中心とする星形領域とし，$f : U \to \mathbb{C}$ を解析関数とする．このとき，$f(z)$ は U で積分可能であり，関数

$$F(z) = \int_{\overline{z_0 z}} f(z)dz$$

は U において $f(z)$ の原始関数である．さらに，そのとき U の任意の閉曲線 γ に対して次が成り立つ．

$$\int_\gamma f(z)dz = 0.$$

（証明） 任意の三角形の境界に対して，$\int_{\partial\triangle} f(z)dz = 0$ が成り立つ．このとき，定理は積分可能性に対する判定条件より直接導かれる．■

星状領域に対するコーシーの積分定理の例をあげよう．$\mathbb{C}^- = \{z \in \mathbb{C}; z \notin \mathbb{R}$ または $z \in \mathbb{R}, z > 0\}$ とする．$\mathbb{C}^-$ は 1 を中心とする星状領域である．$f(z) = 1/z$ とおく．$f(z)$ は解析的であって，$\int_{\overline{1z}} \frac{1}{z} dz$ は $f(z)$ の原始関数である．

1 から $z = re^{i\theta}$ への曲線を次のように選ぶ．はじめに，$\mathbb{R}$ 上を 1 から r への線分をとり，次に $z = re^{i\phi}$ に沿って r から z へ円弧をとる．このとき，

$$\int_{\overline{1z}} \frac{dz}{z} = \int_1^r \frac{dt}{t} + \int_0^\theta \frac{ire^{it}}{re^{it}} dt = \log r + i\theta.$$

ここで，対数は $\mathbb{C}^-$ における複素対数関数の主枝である．

コーシー・グールサの定理を使えば，コーシーの積分定理とリウヴィルの定理は第 5 章のように証明される．このことから，代数学の基本定理の第 2 の証明を得た．付録 C において，複素解析学の他のいくつかの結果を用いてさらに 3 つの解析的証明を与える．

付録C

代数学の基本定理のさらに3つの複素解析的証明

第 5 章で与えた代数学の基本定理の複素解析的証明はリウヴィルの定理 (定理 5.4.1) に基礎をおいていた．この付録においては，この定理に基礎をおかないさらに 3 つの証明を与える．このために，準備として次の 2 つの補題が必要である．最初の補題はコーシーの積分定理の直接的な結果である．

補題 C.1（複素積分に対する平均値の定理と不等式）$U \subset \mathbb{C}$ を開集合，$f : U \to \mathbb{C}$ を解析関数とする．$B = B_r(z_0)$ を U に含まれている中心 z_0 で半径 $r > 0$ の円板とする．このとき，∂B に対する媒介変数表示 $\gamma(t) = z_0 + re^t$, $(0 \le t \le 2\pi)$ を用いて次の 2 つの式を得る．

$$f(z_0) = \frac{1}{2\pi}\int_0^{2\pi} F(z_0 + re^{it})dt \quad （平均値の定理）$$

$$|f(z_0)| \le \max_{z\in\partial B} |f(z)| \quad （平均値の不等式）$$

第 2 番目のものは **growth lemma** と呼ばれている次の補題である．

補題 C.2（growth lemma）$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ $(a_n \ne 0)$ を次数 $n > 1$ の複素多項式とする．このとき，適当な数 $R \ge 1$ が存在して，$|z| \ge R$ なる $z \in \mathbb{C}$ に対して次が成り立つ．

$$\frac{1}{2}|a_n||z|^n \le |p(z)| \le 2|a_n||z|^n.$$

特に，$|z| \to \infty$ ならば $|p(z)| \to \infty$ となる．

（証明） $r(z) = |a_0| + |a_1||z| + \cdots + |a_{n-1}||z|^{n-1}$ とおけば，三角不等式より

$$|a_n||z|^n - r(z) \le |p(z)| \le |a_n||z|^n + r(z).$$

$|z| \ge 1$ のとき，$i < n$ に対して $|z|^i \le |z|^{n-1}$ であるから，$k = \sum_{i=0}^{n-1} |a_i|$ とおけば $r(z) \le k|z|^{n-1}$ が成り立つ．したがって，

$$R = \max\{1, 2k|a_n|^{-1}\}$$

とすれば，求める式が得られる．■

さて，今やいよいよ 3 つの新しい証明を与えることができる．再び，任意の定数でない複素多項式は複素数の根をもつことを証明しよう．

第 7 の証明

$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ を次数 $n > 1$ の複素多項式とし，$p(z)$ は $\mathbb{C}$ において零点をもたないと仮定する．第 3 章におけるように (3.4.1 参照)，$\overline{p}(z) = \overline{a_0} + \overline{a_1} z + \cdots + \overline{a_n} z^n$ とする．任意の $z \in \mathbb{C}$ に対して，$\overline{p}(\overline{z}) = \overline{p(z)}$ であるから，$g(z) = p(z)\overline{p}(z)$ は次数 $2n$ であり，また，$\mathbb{C}$ に零点をもたない．さらに，$g(x) = |p(x)|^2 > 0$ $(x \in \mathbb{R})$ が成り立っている．

$\dfrac{1}{g(z)}$ は $\mathbb{C}$ で正則であるから，コーシーの定理によって，$r > 0$ に対して

$$0 = \int_{-r}^{r} \frac{dx}{|p(x)|^2} + \int_{\gamma_r} \frac{dz}{g(z)} \tag{C.1}$$

が成り立つ．ただし，$\gamma_r(t) = re^{it}$, $(0 \le t \le \pi)$ は 0 を中心として半径 r の半円である．これを図 C.1 において図示する．

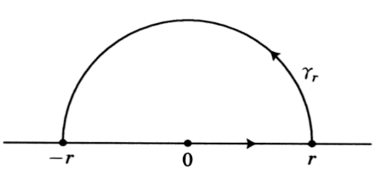


図 C.1　第 7 の証明における半円

補題 C.2 によって，r を十分大きくするとき，$|z| \geq r$ に対して，$M = 4|a_n|^{-2}$ とおけば

$$|g(z)|^{-1} \leq M|z|^{-2n}$$

が成り立つ．このとき，そのような r に対して次の不等式を得る．

$$\left|\int_{\gamma_r} \frac{dz}{g(z)}\right| \leq \max_{\gamma_r}\left|\frac{1}{g(z)}\right|\pi r \leq \pi M r^{-(2n-1)}.$$

よって，$n > 1$ であるから

$$\lim_{r\to\infty}\int_{\gamma_r}\frac{dz}{g(z)} = 0.$$

したがって，(C.1) より

$$\lim_{r\to\infty}\int_{-r}^{r}\frac{dx}{|p(x)|^2} = 0$$

でなければならない．ところが，$|p(x)|^2 > 0$ であるから，これは不可能である．■

第 8 の証明

$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ を次数 $n > 1$ の複素多項式とし，$p(z)$ は $\mathbb{C}$ において零点をもたないと仮定する．$|f(z)| = \dfrac{1}{p(z)}$ は $\mathbb{C}$ で解析的であるから，平均値の不等式によって，0 を中心とする半径 $r > 0$ の円板 $B_r(0)$ に対して

$$f(0) \leq \max_{z\in\partial B_r}|f(z)|$$

が成り立つ．補題 C.2 によって，$\lim_{z\to\infty}|f(z)| = 0$ であるから，$f(0) = 0$ となる．ところが，これは $f(0) = p(0)^{-1} \neq 0$ であることに矛盾する．■

最後の証明は**最大最小の原理** に基づいている．これは第 5.5 節において言及しておいた．これは再び，コーシーの積分公式の結果である．ここでは，これを再録し，2 つの重要な系を与えて，それから第 9 の証明を与える．

定理 C.1（最大値の原理）$f(z)$ は領域 U において定数でない解析関数とする．このとき，$z_0 \in \mathbb{C}$ の $\mathbb{C}$ におけるすべての近傍は $|f(z)| > |f(z_0)|$ を満たす点 z を含む．

系 C.1（最大値の原理）$f(z)$ は領域 U において解析関数とする．$f(z)$ に対して局所的に最大値となっている点 $z_0 \in \mathbb{C}$ が存在すると仮定する，すなわち，$z \in B_\epsilon(z_0)$ に対して $|f(z)| \leq |f(z_0)|$ を満たす円板 $B_\epsilon(z_0) \subset \mathbb{C}$ が存在すると仮定する．このとき，$f(z)$ は U において定数となる．

系 C.2（最小値の原理）$f(z)$ は領域 U において解析関数とする．$f(z)$ に対して局所的に最小値となっている点 $z_0 \in \mathbb{C}$ が存在すると仮定する，すなわち，$z \in B_\epsilon(z_0)$ に対して $|f(z_0)| \leq |f(z)|$ を満たす円板 $B_\epsilon(z_0) \subset \mathbb{C}$ が存在すると仮定する．このとき，$f(z) = 0$ であるかまたは $f(z)$ は U において定数となる．

第 9 の証明のためにもう 1 つ別の事実が必要である．体上の多項式は有限個の零点しかもたないので (第 3 章参照), 定数でない複素多項式 $p(z)$ はいかなるところにおいても局所的に定数にはならない．すなわち，どんな開集合 U に対しても $p(z)$ は U 上で定数とはならない．なぜならば，任意の $z \in U$ に対して $p(z) = c$ ならば，そのとき多項式 $g(z) = p(z) - c$ は無限に多くの零点をもつことになるからである．

第 9 の証明

$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ を次数 $n > 1$ の複素多項式とする．任意の $r > 0$ に対して，$U_r = B_r(0)$ を 0 を中心とする半径 r の閉じた円板とする．U_r はコンパクト集合であり，$p(z)$ は連続であるから，$|p(z)|$ は適当な点 $z_r \in U_r$ で最小値をとる．$|z| \to \infty$ ならば $|p(z)| \to \infty$ であるから，この最小値を与える点 z_R が U_R の内部にあるように十分大きく R を選ぶことができる．このことを見るために，$|z| > s$ に対して $|p(z)| > |a_0| = |p(0)|$ となるように $s > 0$ を選ぶ．そして，$R > s$ なる R を選ぶ．そのとき，U_R の境界上で $|p(z)| > |p(0)|$ が成り立つ．したがって，コンパクト集合 U_R 上の最小値はその内部になければならない．

以上より，$z_R \in$ (U_R の内部) であって，すべての $z \in U_R$ に対して $|p(z_R)| \leq |p(z)|$ が成り立つ．z_R は内部にあるから，ある $\epsilon > 0$ が存在して，z_R を中心とする半径 ϵ の閉じた円板 $U_1 = B_\epsilon(z_R)$ が U_R に含まれている．ところが，$p(z)$ はいたるところで解析的であるから，U_1 上で解析的であり，さらに，任意の $z \in U_1$ に対して $|p(z_R)| \leq |p(z)|$ が成り立つ．最小値の原理より，

$p(z_R) = 0$ であるか，または $p(z)$ は U_1 上で局所的に定数である．上で述べたように，定数でない多項式はどの点においても局所的に定数ではない．したがって，$p(z_R) = 0$ となる．■

付録 D

代数学の基本定理のさらに 2 つの位相的証明

この最後の付録 D において，回転数に依存しているさらに 2 つの位相的証明を与える．最初のものは第 9 章において与えたブラウアー次数を用いた証明の 1 つの変形であり，もう一つのものは第 8 章の冒頭において説明した単純な回転数の形式的な表現である．

単位円 S^1 における**ループ**とは $f(0) = f(1)$ を満たす関数 $f : [0,1] \to S^1$ であったことを思い出そう．第 9 章において見たように，基本群 $\prod_1(S^1)$ は無限巡回群である．ゆえに，単位円 S^1 におけるループに対して，その**写像度**あるいは**回転数**と呼ばれる整数 m が対応していた．これは z が S^1 における f の像の上を動くとき，z の偏角の変化に $1/2\pi$ をかけたものである．f が解析的であれば，これは $\dfrac{1}{2\pi}\displaystyle\int_{Im(f)}\dfrac{dz}{z}$ に等しい．g が S^1 において f にホモトープならば，f と g は同じ写像度をもつ．$h = fg$ ならば，$\deg(h) = \deg(f) + \deg(g)$ が成り立つ．ただし，$\deg f$ は f の写像度を表すものとする．$z \to z^n$ によって与えられる写像 $S^1 \to S^1$ は明らかに写像度 n である．

集合 $\mathbb{C} - \{0\}$ は環状の領域にホモトープであり，S^1 に変形することができる．ゆえに，$\mathbb{C} - \{0\}$ の任意のループは S^1 上のループにホモトープであり，したがってある写像度をもつ．これを 0 をまわるループの写像度または回転数と呼ぶ．一般に，$z_0 \in \mathbb{C} - \{0\}$ ならば，z_0 をまわるループ $f(t)$ の写像度または回転数はループ $g(t) = f(t) - z_0$ の写像度のことである．ホモトピーや写像度についての事柄はすべて $\mathbb{C} - \{0\}$ における一般のループに移行することができる．代数学の基本定理の 10 番目の証明は次の重要な定理と関係して

いる．

定理 D.1（ルーシェの定理）$f, g : [0,1] \to \mathbb{C}$ をすべての t に対して $|g(t)| < |f(t)|$ を満たすループとする．このとき，f と $f+g$ は同じ写像度をもつ．

（**証明**）与えられた条件より f と $f+g$ は $\mathbb{C}-\{0\}$ 上の写像である．$H(t,u) = f(t)+ug(t)$ を考える．$H(t,u)$ は $H(t,0) = f(t)$ から $H(t,1) = f(t)+g(t)$ へのホモトピーである．さらに，$f(t), g(t)$ についての条件は $H(t,u) = 0$ なる (t,u) の選択の余地はないことを保証している．ゆえに，$H(t,u)$ は $\mathbb{C}-\{0\}$ におけるホモトピーである．したがって，f と $f+g$ はホモトープであるから，同じ写像度をもつ．■

第 10 の証明

$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ $(a_n \neq 0)$ を複素多項式とする．任意の $r \geq 0$ に対して $p_r(z) = p(rz)$ によって $p_r : S^1 \to \mathbb{C}$ を定義する．このとき，任意の r に対して写像 $H(t,u) = p(zru)$ は $\mathbb{C}$ における p_r から p_0 へのホモトピーである．多項式 $p(z)$ が 0 にならなければ，これは $\mathbb{C}-\{0\}$ におけるホモトピーとなり，したがって，p_r と p_0 は同じ写像度をもつ．今 p_0 は定数であるから，写像度は 0 である．p_R が写像度 n をもつような R が存在することを示そう．このとき，$n = 0$ となり，したがって，$p(z)$ は定数となる．

$R > \max(1, \sum_{k=0}^{n-1} \dfrac{|a_k|}{|a_n|})$ とする．このとき，$|z| = R$ なるすべての z に対して次が成り立つ．

$$|\sum_{k=0}^{n-1} a_k z^k| \leq \sum_{k=0}^{n-1} |a_k||z|^k \leq (\sum_{k=0}^{n-1} |a_k|)|z|^{n-1} < |a_n||z|^n.$$

ルーシェの定理より，p_R は z を $a_n R^n z^n$ へ移す S^1 上の関数と同じ写像度をもち，この関数は写像度 n をもつ．p_R と p_0 は同じ写像度をもつので，$n = 0$ である．したがって，$p(z)$ が根をもたなければ $p(z)$ は定数である．■

最後の証明は上の証明に似ているが，ルーシェの定理は使わない．

第 11 の証明

前と同様に，$p(z) = a_0 + a_1 z + \cdots + a_n z^n$ $(a_n \neq 0)$ を複素多項式とする．一般性を失わずに，$a_n = 1$ と仮定してよい．任意の $r \geq 0$ に対して

$$p_r(t) = \frac{|p(r)|}{p(r)} \frac{p(re^{2\pi it})}{|p(re^{2\pi it})|}. \tag{D.1}$$

とする．$p(z)$ が根をもたなければ，$(D.1)$ における 2 つの分数のそれぞれは矛盾なく定義され，その絶対値は 1 である．したがって，任意の $r \geq 0$ と任意の $t \in [0,1]$ に対して $p_r(t) \in S^1$ となる．さて，$p_0(t)$ は S^1 の定数であるループである．最初の分数はループ $p_r(t)$ の始点を与え，一方第 2 の分数は $\mathbb{C} - \{0\}$ におけるループ $p(re^{2\pi it})$ を S^1 の上に射影する．

次に，$H(t,u) = p_{ru}(t)$ とおく．これは S^1 において，$p_r(t)$ から $p_0(t)$ へのホモトピーを与える．ゆえに，任意の r に対して，$p_r(t)$ と $p_0(t)$ は写像度 0 をもつ．$p_R(t)$ が写像度 n をもつような値 R が存在することを示す．

$S = \max(1, |a_1|, \ldots, |a_{n-1}|)$, $R = (n+1)S$ とする．$f(t) = Re^{2\pi it}$ を中心が 0 で半径 R の円とし，$q(z) = z^n$ とおく．このとき，$q(f(t)) = R^n e^{2\pi nit}$ は原点のまわりの半径 R の円上で回転数 n をもつループである．任意の t に対して $q(f(t))$ から $p(f(t))$ への距離を考える．このとき，

$$\begin{aligned}
|q(f(t)) - p(f(t))| &= |f(t)^n - (f(t)^n + a_{n-1} f(t)^{n-1} + \cdots + a_0)| \\
&\leq |a_{n-1} f(t)^{n-1}| + \cdots + |a_0| \\
&\leq |a_{n-1}||f(t)^{n-1}| + \cdots + |a_0| \\
&\leq |a_{n-1}| R^{n-1} + \cdots + |a_0| \\
&\leq \frac{R}{n+1} R^{n-1} + \cdots + \frac{R}{n+1} \leq \frac{n}{n+1} R^n < R^n.
\end{aligned}$$

この式は任意の t に対して $p(f(t))$ が $q(f(t))$ を中心とする半径 R^n の円板の中にあるということを表している．特に，そのとき，原点を通らない $q(f(t))$ から $p(f(t))$ への線分が存在する．これは本質的に第 8 章で述べた同伴者の定理の 1 つの変形である．これは，関数 $K(t,u) = uq(f(t)) + (1-u)p(f(t))$ は $u \in [0,1], t \in [0,1]$ に対して，決して 0 にはならないことを主張している．

$$H(t,u) = \frac{|K(0,u)|}{K(0,u)} \frac{K(t,u)}{|K(t,u)|}$$

とおく．直接的な計算によって，$H(t,0)=p_R(t)$, $H(t,1)$ は回転数 n のループ，$r(t)=e^{2\pi int}$ であり，そして任意の u に対して $H(0,u)=1$ となることがわかる．ゆえに，$H(t,1)$ は S^1 において $H(t,0)=p_R(t)$ から $H(t,1)=r(t)$ へのホモトピーである．したがって，$p_R(t)$ は写像度 n をもつ．それは写像度 0 をもっていることはわかっているので，$n=0$ でなければならない．以上より，$p(z)$ は定数であることがわかる．■

参考文献および引用文献

引用文献

[A] L. Ahlfors, *Complex Analysis,* McGraw-Hill, 1966.

[G] N. Gupta, *The Burnside Problem,* The American Mathematical Monthly, 1991.

[H-Y] J.G. Hocking and G.S. Young, *Topology,* Addison-Wesley, 1961.

[R] R. Remmert, *Fundamentalsatz der Algebra,* Zahlen, by H.D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, Sprinder-Verlarg, 1983.

[Ro] J. Rotman, *Theory of Groups,* W.C. Brown-3rd Edition, 1988.

[U] J.V. Upsensky, *Theory of Equations,* McGraw-Hill, 1948.

訳者による補遺

[1] 新妻弘，木村哲三：「群・環・体入門」，共立出版，2001.

[2] ロットマン：「ガロア理論入門」，シュプリンガー東京，2000.

[3] 永田雅宜：「可換体論」，裳華房，1985.

[4] ファン・デル・ヴェルデン 著，加藤明文 訳：「代数学の歴史」，現代数学社，1994.

[5] アールフォース 著，笠原乾吉 訳：「複素関数論」，現代数学社，2000.

[6] 高木貞治：「解析概論」，岩波書店，1970.

[7] 松阪和夫：「集合・位相入門」，岩波書店，1997.

[8] 河田敬義，三村征雄：「現代数学概説 II」，岩波書店，1965.

参考文献

複素解析学

L. Ahlfors, *Complex Analysis,* McGraw-Hill, 1966.

E.A. Grove and G. Ladas, *Introduction to Complex Variables*, Houghton-Mifflin, 1974.

R. Remmert, *Funktionentheorie 1 and 2*, Springer-Verlag, (1984, 1991).

一般代数とガロア理論

M. Artin, *Algebra*, Prentice-Hall, 1991.

H. Edward, *Galois Theory*, Springer-Verlag, 1984.

J.B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley-5th Edition-, 1993.

S. Lang, *Algebra*, Addison-Wesley, 1984.

P.J. McCarthy, *Algebraic Extensions of Fields*, Dover, 1976.

B.L. Van Der Waerden, *Modern Algebra*, Ungar Publishing, New York-third printing, 1964.

位相と代数的位相

J.G. Hocking and G.S. Young, *Topology,* Addison-Wesley, 1961.

K.L. Kelly, *General Topology*, Van Nostrand, 1955.

K.H. Mayer, *Algebraische Topologie*, Birkhauser, 1989.

W.S. Massey, *Algebraic Topology: an introduction*, Harcourt, Brace and World, 1967.

J.R. Munkres, *Topology: A First Course*, Prentice-Hall, 1975.

R. Stoecker and H. Zieschang, *Algebraische Topologie*, B.G. Teubner, 1988.

ガウスのオリジナルの証明

C.F. Gauss, *First Proof*, docotoral thesis Helmstadt-(in-Werke, 3, 1-30), 1799.

C.F. Gauss, *Second Proof*, Comm. Soc. Goett. 3, 1814/15, 107-142.

C.F. Gauss, *Third Proof*, Comm. Soc. Goett. 3-(in-Werke, 3), 1816, 59-64.

C.F. Gauss, *Fourth Proof*, Abhand. der Ges. der Wiss. zu Goett. 4, 1848/50, 3-34.

索 引

【あ行】

アーベル群（abelian group）, 6, 102, 124
アルキメデス的（Archimedean）, 10
アルティン（Artin）, 137

位数（order）, 102, 124
位相（topology）, 171
位相空間（topological space）, 171
位相不変量（topological invariant）, 179
一意分解整域（unique factorization domain）, 28
位置解析（analysis situs）, 161
一様連続（uniformly continuous）, 170
イデアル（ideal）, 96
因子群（factor group）, 147
因数（factor）, 29

海（sea）, 218
ウリゾーンの埋蔵定理（Urysohon embedding theorem）, 174

円積問題（square the circle）, 152
円の花束（bouquet of n circles）, 194

オイラーの等式（Euler's identity）, 19
オイラーの魔法の等式（Euler's magic formula）, 19

【か行】

海岸線（shore）, 218
開基底（open base, open basis）, 174
開球体（open ball）, 168
開近傍（open neighborhood）, 169
開写像（open mapping）, 172
開集合（open set）, 44, 161, 168, 171
階数 n の自由群（free group of rank n）, 194
階数 n の自由アーベル群（free abelian group of rank n）, 182
解析的（正則）(analytic, regular, holomorph）, 47
回転数（winding number）, 158, 159, 234
開被覆（open cover）, 175
可解群（solvable group）, 147
可換（交換可能）（commutative）, 186
核（kernel）, 129
各元を固定（fix each element）, 105
拡大（extension）, 88
拡大（magnification）, 58
拡大次数（degree of the extension）, 9
拡大体（extension field, field extension）, 8, 88
角を保存（preserve angle）, 56
角の 3 等分（trisect an angle）, 152
カルダノの公式（Caldano's formula）,

146
ガロア拡大（Galois extension）, 123, 134
ガロア群（Galois group）, 123
ガロア理論の基本定理（fundamental theorem of Galois theory）, 140
環（ring）, 6
関係（relation）, 105
完全（exact）, 66
完全正則空間（completely regular space）, 173
完備（complete）, 11

基礎体（ground field）, 89
奇置換（odd permutation）, 157, 196
基底（basis）, 182
基本群（fundamental group）, 180, 192
既約多項式（irreducible polynomial）, 29
境界（boundary）, 170, 198
境界群（boundary group）, 202, 203
境界作用素（boundary operator）, 203
境界準同型写像（boundary homomorphism）, 202
共役（conjugate）, 111, 138
共役調和関数（conjugate harmonic function）, 54
極形式（polar form）, 17
極限点（limit point）, 170
極座標（polar cordinates）, 16
曲線（curve）, 55
虚部（imaginary part）, 43
距離（metric）, 164
距離関数（distance function）, 164
距離空間（metric space）, 165
距離づけ可能（metrizable）, 172, 174
距離づけ可能性（metrizability）, 172

空間のホモトピー類（homotopy classes of spaces）, 189
偶置換（even permutation）, 157, 196
区間縮小法の原理（nested intervals property）, 11
区分的に連続的微分可能（piecewise continuously differentiable）, 221
グリーンの定理（Green's theorem）, 68
グールサの積分補助定理（integral lemma of Goursat）, 225
クロネッカーの定理（Kronecker's theorem）, 96

係数（coefficient）, 25
係数（modulus）, 17
経路に独立（independent of path）, 66, 71
原始関数（primitive function）, 222
原始元（primitive element）, 134
原始元定理（primitive element theorem）, 134

原始多項式（primitive polynomial）, 110

語（word）, 194
交換子（commutator）, 156, 186
交換子部分群（commutator subgroup）, 186
交代群（alternating group）, 157
互換（transposition）, 157
弧状連結（path-connected）, 192
コーシー・グールサの定理（Cauchy-Gursat theorem）, 76
コーシー・シュワルツの不等式（Cauchy-Schwartz inequality）, 167
コーシーの積分公式（Cauchy integral formula）, 77,78
コーシーの定理（Cauchy's theorem）, 76
コーシーの評価式（Cauchy's estimate）, 81
弧状連結（path-connected）, 220
コーシー列の収束性（Cauchy sequence property）, 11
固定（fix）, 126
根（root）, 28
コンパクト（compact）, 174, 175
コンパクト集合（compact set）, 161

コンパクト性（compactness），172, 174

【さ行】

最高次係数（leading coefficient），25
最小整多項式(entire minimal polynomial)，111
最小多項式（minimal polynomial），110
最小値の原理（minimum principle），232
最小分解体（splitting field），100
最大公約数 (gcd)（greatest common divisor），29
最大最小の原理（maximum minimum modulus principle），231
最大値・最小値の定理（extreme value theorem），37
最大値定理（maximum modulus theorem），84
最大値の原理（maximum modulus principle），85, 231
最大値の原理（maximum principle），232
作図可能（constructible），149
作図可能数（constructible number），149
三角形分割（triangulation），180, 200
三分法（trichotomy law），10

時間媒介変数空間（time parameter space），188
自己同型群（automorphism group），125
指数（index），127
実解析関数（real analytic function），81
実数（real numbers），7
実部（real part），43
写像（mapping），43
写像度（degree of mapping），208, 234
斜体（skew field），153
周回積分（commplex contour integral），73
重根（multiple root），132
収縮可能（contractible），189
重複度（multiplicity），34, 132
巡回群（cyclic group），182
巡回置換（cycle），156
順序体（orderd field），10
準同型写像（homomorphism），12, 124
準同型像（homomorphic image），130
剰余群（factor group, quotient group），129
剰余類（coset），97
除法の定理（division algorithm），29
ジョルダンの曲線定理（Jordan curve theorem），67
シローの定理（Sylow theorem），131

整域（integral domain），26
整関数（entire function），47
正規化（normalize），127
正規拡大（normal extension），132
正規化群（normalizer），127
正規空間（normal space），173
正規部分群（normal subgroup），127
正規列（normal series），147
制限完備性（least upper bound property），11
星状（starlike），222
星状領域（starlike domain），222
星状領域に対するコーシー・グールサの定理（Cauchy-Goursat theorem for star domains），227
生成される（generated），105
生成元（generator），105
正則（regular），55
正則曲線（regular curve），55
積分可能（integrable），222
積分可能性に対する三角形判定法（triangle criterion for integrability），224
積分可能判定条件（criteria for integrability），222
ゼロ（zero），28
ゼロ多項式（zero polynomial），25

線積分（line integral）, 62
全微分（total differential）, 65

素イデアル（prime ideal）, 120
像（image）, 129
素数 p を法とする剰余類（integers modulo any prime p）, 7

【た行】

第 1 次微分形式（first order differential form）, 65
第 1 同型定理（first isomorphism theorem）, 130
対称（symmetric）, 105
対称群（symmetric group）, 102, 104, 124
対称式（symmetric polynomial）, 105
対称式の基本定理（fundamental theorem of symmetric polynomials）, 107
代数拡大（algebraic extension）, 89
代数学の基本定理（fundamental theorem of algebra）, 38, 83, 108, 145, 159, 211
代数的（algebraic）, 9, 89
代数的位相幾何学（algebraic topology）, 162, 179
代数的位相不変量（algebraic topological invariant）, 179
代数的整数（algebraic integer）, 111
代数的閉体（algebraically closed field）, 88, 101
代数的閉包（algebraic closure）, 95, 101
第 2 可算空間（second countable space）, 174
代入（substitution process）, 27
互いに素（relative prime）, 30
多角形的曲線（polygonal cueve）, 220
多元体（division algebra）, 153
多項式（polynomial）, 25
多項式のガロア群（Galois group of the polynomial）, 137
多項式の共役（conjugate of a polynomial）, 35
単位元をもつ可換環（commutative ring with an identity）, 6
単項式（pieces, monomial）, 116
単根（simple root）, 132
単純拡大（simple extension）, 92
単純群（simple group）, 128
単純閉曲線（simple closed curve）, 67
単体（simplex）, 180, 196
単体的複体（simplicial complex）, 180, 199, 200
単体分割（simplicial decomposition）, 180, 200
単連結（simply connected）, 44, 192

置換（permutation）, 102, 124
中間体（intermediate field）, 89
中間値の定理（intermediate value theorem）, 11
中心（center）, 222
超越拡大（transcendental extension）, 89
超越数（transcendental number）, 9
超越的（transcendental）, 10, 89
調和関数（harmonic function）, 53
直積（direct product）, 181

定数多項式（constant polynomial）, 25
点（point）, 171
点集合の位相（point set topology）, 162

同相写像（homeomorphism）, 172
等角（conformal）, 56
等角写像（conformal mapping）, 56
同型（isomorphic）, 12
同型写像（isomorphism）, 12, 124
同相空間（homeomorphic spaces）, 172
同値（equivalent）, 73
閉じた道（closed path）, 189
凸胞体（convex hull）, 196
ド・モアブルの定理（DeMoivre's theorem）, 20

【な行】

内積（inner product），166
内積空間（inner product space），166
内点（interior point），170

ねじれがない（torsion-free），183
ねじれ部分群（torsion subgroup），183

ノルム空間（norm space），166

【は行】

ハイネ・ボレル（Heine-Borel），175
ハウスドルフ空間（Hausdorff space），173
バーンサイドの問題（Burnside problem），184

左剰余類（left coset），126
被覆空間（covering space），195
被覆写像（covering map），195
微分可能（differentiable），47, 55
微分可能な曲線（differentiable curve），55
微分係数（derivative），47
表現（presentation），105
標数（characteristic），132
非連結（disconnection），175

複素関数（complex function），43
複素積分に対する平均値の定理と不等式（mean value theorem and inequality for complex integrals），229
複素線積分（complex line integral），73
複素変数（complex variables），43
不動点（fixed point），209
部分群（subgroup），102, 124
部分体（subfield），8
部分被覆（subcover），175
不変性定理（invariance theorem），203
普遍被覆空間（universal covering space），195
ブラウアー次数（Brouwer degree），208
ブラウアーの不動点定理（Brouwer fixed point theorem），209
分離拡大（separable extension），132
分離的（separable），132
分類問題（classification problem），172

閉集合（closed set），44, 161, 168, 171
ベキ根によって可解（solvable by radicals），147
ベキ根による F の拡大（extension of F by radicals），147
ベクトル空間（vector space），9
ベッチ数（Betti number），185
偏角（argument），17
変換（transformation），43

方向（direction），55
方程式のガロア群（Galois group of the equation），123
ホモトピー（homotopy），188
ホモトピー同値（homotopy equivalent），189
ホモトピー不変量（homotopy invariant），180, 189
ホモトピー理論（homotopy theory），180
ホモトープ（homotopic），180, 188, 189
ホモトープ同値（homotopically equivalent），180
ホモローグ（homologous），203
ホモロジー群（homology group），202, 203
ホモロジー理論（homology theory），180

【ま行】

右剰余類（right coset），126
道（path），189

向きのついた q 単体 (oriented q-simplex)，196, 197

モニック多項式（monic polynomial），

25
モレラの定理 (Morera's theorem), 84

【や行】

有界 (bounded), 44
有限群 (finite group), 102, 124
有限次拡大 (finite extension), 88
有限生成 (finitely generated), 184
有限生成アーベル群の基本定理 (fundamental theorem for finitely generated abelian groups), 185
有限単純群の分類定理 (classification theorem for finite simple groups), 128
有理数 (rational numbers), 7
ユークリッド空間 (Euclidean space), 165
ユークリッドの互除法 (Euclidean algorithm), 30
ユークリッドの補題 (Euclid's lemma), 31

【ら行】

ラグランジュの定理 (Lagrange's theorem), 127
ラプラスの方程式 (Laplace's equation), 53
リウヴィルの定理 (Liouville's theorem), 82
陸 (land), 218
離散位相 (discrete topology), 171
立体射影 (stereographic projection), 209
立方体倍積問題 (double the cube), 152
リーマン球面 (Riemann sphere), 210
領域 (domain), 44
輪体 (cycle), 202
輪体群 (cycle group), 202, 203
ルーシェの定理 (Rouche's theorem), 235
ループ (loop), 189, 234
零因子 (zero divisor), 26
連結 (connected), 44
連結集合 (connected set), 161
連結性 (connectedness), 172, 175
連結成分 (connected component), 204
連続 (continuous), 46, 163, 164, 168
連続関数 (continuous function), 172
連続写像 (continuous mapping), 172
連続的微分可能 (continuously differentiable), 55

【わ行】

和 (sum), 221
割り切る (divide), 29

【欧文】

1 次因数に分解 (split), 100
1 次結合 (linear combination), 30
2 重積分 (double integral), 62
4 元数体 (quaternion algebra), 154
Aut(R), 125
F-同型写像 (F-isomorphism), 94
n 鎖 (n-dimensional chain), 201
n 鎖加群 (n-dimensional chain group), 201
n 乗根 (n-th root), 20
p-群 (p-group), 185
p-シロー部分群 (p-Sylow subgroup), 130
T_1-空間 (T_1-space), 173

〈訳　者〉

新妻　弘（にいつま　ひろし）
東京理科大学理学部数学科教授・理学博士

木村哲三（きむら　てつぞう）
大東文化大学経済学部現代経済学科教授・理学博士

代数学の基本定理

2002年 2月20日　初版1刷発行
2002年10月10日　初版2刷発行

訳　者　新妻　弘　©2002
　　　　木村哲三

発行者　南條光章

発行所　**共立出版株式会社**
東京都文京区小日向4-6-19
電話　03-3947-2511（代表）
郵便番号　112-8700
振替口座　00110-2-57035
URL http://www.kyoritsu-pub.co.jp/

印　刷　啓文堂
製　本　関山製本

社団法人
自然科学書協会
会員

検印廃止
NDC 411

ISBN 4-320-01689-0

Printed in Japan